Приложение 1.

УТВЕРЖДЕНО
Распоряжением Администрации
Качканарского городского округа
Свердловской области
от 29.09.2023 № 83
«Об информационной безопасности
(защите информации) в Администрации
Качканарского городского округа
Свердловской области»

Положение
об информационной безопасности (защите информации) Администрации Качканарского городского округа Свердловской области

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об информационной безопасности (защите информации) Администрации Качканарского городского округа Свердловской области (далее - Положение, Организация) разработано в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

- «ГОСТ Р 51583-2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (утвержден и введен в действие Приказом Росстандарта от 28.01.2014 № 3-ст);

- «ГОСТ Р 56545-2015. Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей» (утвержден и введен в действие Приказом Росстандарта от 19.08.2015 № 1180-ст);

- «ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят и введен в действие Постановлением Госстандарта Российской Федерации от 09.02.1995 № 49);

- «ГОСТ Р 56938-2016. Национальный стандарт Российской Федерации. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения» (утвержден и введен в действие Приказом Росстандарта от 01.06.2016 N 457-ст);

- «ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» (утв. Приказом Ростехрегулирования от 27.12.2007 № 513-ст);

- «ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции» (утвержден и введен в действие Приказом Росстандарта от 01.12.2011 № 683-ст);

- и иными нормами действующего законодательства Российской Федерации.

1.2. Положение обязательно к исполнению всеми работниками Организации.

1.3. Положение подлежит применению по месту нахождения учреждения - адрес: Свердловская область, г.Качканар, ул.Сверлова, д. 8.

1.4. Сокращения Положения:

- ИС - информационные системы;
- СВТ - средства вычислительной техники;
- НСД - несанкционированный доступ;
- КСЗ - комплекс средств защиты;
- ЗИ - защита информации;
- ВВС - виртуальные вычислительные системы;
- ПРД - правила разграничения доступа;
- ГРИИБ - группа реагирования на инциденты информационной безопасности.

1.5. Подразделением, отвечающим за реализацию настоящего Положения, является отдел по организационной работе Администрации Качканарского городского округа Свердловской области (далее - Служба).

1.6. Информационная безопасность обеспечивается реализацией следующих мер:

1.6.1. Выполнение технических требований.

1.6.2. Идентификация уязвимостей.

1.6.3. Защита при использовании технологий виртуализации.

1.6.4. Применение системы менеджмента инцидентов информационной безопасности.

1.6.5. Создание структурных подразделений, обеспечивающих информационную безопасность.

1.6.6. Обучение работников Организации приемам информационной безопасности. Требование от работников их выполнения.

1.6.7. Использование КСЗ.

1.6.8. Мониторинг и проверка эксплуатации комплекса программных и технических средств и услуг.

1.6.9. Подготовка предложений по финансированию мероприятий по защите информации.

1.6.10. Оборудование помещений, предназначенных для размещения средств обработки информации ИС, системами инженерно-технического обеспечения (вентиляции, теплоснабжения, кондиционирования, охраны, сигнализации, пожаротушения, энергообеспечения) в соответствии с требованиями по защите информации.

1.6.11. Организация технического обслуживания и ремонта средств вычислительной техники, предназначенных для обработки информации ограниченного доступа, с учетом требований по защите информации.

II. ЗАЩИТА ИНФОРМАЦИИ

2.1. Защита информации в Организации представляет собой принятие правовых, организационных и технических мер, направленных:

1) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2.2. Организация как обладатель информации и/или оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязана обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации;

8) документирование доказательств неправомерного доступа к компьютерной информации, создания, использования и распространения вредоносных компьютерных программ, нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, нарушения правил защиты информации, незаконной деятельности в области защиты информации, разглашения информации с ограниченным доступом, воспрепятствования уверенной работе сайтов в сети Интернет, нарушения требований законодательства о хранении документов и информации, содержащейся в информационных системах;

9) сопровождение исполнения заключенных Организацией договоров на закупку товаров, работ и услуг по темам развития и обеспечения защиты информации;

10) ведение реестра приобретенных средств защиты информации;

11) проведение служебных расследований по фактам нарушения требований защиты информации;

12) взаимодействие с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации по вопросам защиты информации в Организации;

13) обеспечение устойчивости и адаптивности ИС;

14) финансирование мероприятий по защите информации в Организации;

15) закупка товаров, работ и услуг, направленных на обеспечение защиты информации.

2.3. Информация, полученная работниками Организации при исполнении ими профессиональных обязанностей или самой Организацией при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица

федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

2.4. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

2.5. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия Организации или лица, предоставившего такую информацию о себе.

2.6. Порядок доступа к персональным данным граждан устанавливается Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных".

2.7. Документирование информации осуществляется в соответствии с установленными правилами делопроизводства.

2.8. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

2.9. Защита государственной тайны, коммерческой тайны, конфиденциальной информации обеспечивается в соответствии с федеральным законодательством и принятыми локальными нормативно-правовыми актами.

III. ВЫПОЛНЕНИЕ ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ

3.1. Защищенность от НСД к информации при ее обработке СВТ характеризуется тем, что только надлежащим образом уполномоченные лица или процессы, инициированные ими, будут иметь доступ к ознакомлению, созданию, изменению или уничтожению информации.

3.2. Защищенность обеспечивается выполнением трех групп требований к средствам защиты, реализуемым в СВТ:

а) требования к разграничению доступа, предусматривающие то, что СВТ должны поддерживать непротиворечивые, однозначно определенные правила разграничения доступа;

б) требования к учету, предусматривающие то, что СВТ должны поддерживать регистрацию событий, имеющих отношение к защищенности информации;

в) требования к гарантиям, предусматривающие необходимость наличия в составе СВТ технических и программных механизмов, позволяющих получить гарантии того, что СВТ обеспечивают выполнение требований к разграничению доступа и к учету.

3.3. Согласование требований к техническим характеристикам объектов закупки и технических заданий в части обеспечения защиты информации на закупку Организацией товаров, работ и услуг, направленных на развитие и обеспечение функционирования ИС обязательно.

3.4. Подготовка и утверждение требований к техническим характеристикам объектов закупки и технических заданий на закупку Организацией товаров, работ и услуг, направленных на развитие и обеспечение защиты информации, выполняется отделом по организационной работе Администрации Качканарского городского округа Свердловской области.

3.5. Мониторинг и систематическая проверка эксплуатации комплекса программных и технических средств и услуг выполняется отделом по организационной работе Администрации Качканарского городского округа Свердловской области в течение всего срока их использования.

IV. ИДЕНТИФИКАЦИЯ УЯЗВИМОСТЕЙ

4.1. Для однозначной идентификации уязвимости их описание должно включать следующие

элементы:

- идентификатор уязвимости;

- наименование уязвимости;

- класс уязвимости;

- наименование программного обеспечения (ПО) и его версия.

4.2. Для анализа уязвимостей их описание должно включать:

- идентификатор типа недостатка;

- тип недостатка;

- место возникновения (проявления) уязвимости;

- способ (правило) обнаружения уязвимости;

- возможные меры по устранению уязвимости.

4.3. Дополнительная информация об уязвимости может включать:

- наименование операционной системы и тип аппаратной платформы;

- язык программирования ПО;

- служба (порт), которую(ый) используют для функционирования ПО;

- степень опасности уязвимости;

- краткое описание уязвимости;

- идентификаторы других систем описаний уязвимостей;

- дата выявления уязвимости;

- автор, опубликовавший информацию о выявленной уязвимости;

- критерии опасности уязвимости.

- описание реализуемой технологии обработки (передачи) информации;

- описание конфигурации ПО, определяемой параметрами установки;

- описание настроек ПО, при которых выявлена уязвимость;

- описание полномочий (прав доступа) к ИС, необходимых нарушителю для эксплуатации уязвимости;

- описание возможных угроз безопасности информации, реализация которых возможна при эксплуатации уязвимости;

- описание возможных последствий от эксплуатации уязвимости ИС;

- наименование организации, которая опубликовала информацию о выявленной уязвимости;

- дата опубликования уведомления о выявленной уязвимости, а также дата устранения уязвимости разработчиком ПО;

- другие сведения.

4.4. Уязвимости ИС по области происхождения подразделяются на следующие классы:

- уязвимости кода;

- уязвимости конфигурации;

- уязвимости архитектуры;

- организационные уязвимости;

- многофакторные уязвимости.

4.5. Уязвимости ИС по типам недостатков ИС подразделяются на следующие:

- недостатки, связанные с неправильной настройкой параметров ПО;

- недостатки, связанные с неполнотой проверки вводимых (входных) данных;

- недостатки, связанные с возможностью прослеживания пути доступа к каталогам;

- недостатки, связанные с возможностью перехода по ссылкам;

- недостатки, связанные с возможностью внедрения команд ОС;

- недостатки, связанные с межсайтовым скриптингом (выполнением сценариев);

- недостатки, связанные с внедрением интерпретируемых операторов языков программирования или разметки;

- недостатки, связанные с внедрением произвольного кода;

- недостатки, связанные с переполнением буфера памяти;

- недостатки, связанные с неконтролируемой форматной строкой;

- недостатки, связанные с вычислениями;

- недостатки, приводящие к утечке/раскрытию информации ограниченного доступа;

- недостатки, связанные с управлением полномочиями (учетными данными);

- недостатки, связанные с управлением разрешениями, привилегиями и доступом;

- недостатки, связанные с аутентификацией;

- недостатки, связанные с криптографическими преобразованиями (недостатки шифрования);

- недостатки, связанные с подменой межсайтовых запросов;

- недостатки, приводящие к "состоянию гонки";

- недостатки, связанные с управлением ресурсами;

- иные типы недостатков.

4.6. Уязвимости ИС по месту возникновения (проявления) подразделяются на следующие:

- уязвимости в общесистемном (общем) программном обеспечении.

- уязвимости в прикладном программном обеспечении.

- уязвимости в специальном программном обеспечении.

- уязвимости в технических средствах.

- уязвимости в портативных технических средствах.

- уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании.

- уязвимости в средствах защиты информации.

V. ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ

5.1. Виртуализацию проводят в отношении:

- программ;

- вычислительных систем;

- систем хранения данных;

- вычислительных сетей;

- памяти;

- данных.

5.2. К основным объектам защиты при использовании технологий виртуализации относят:

- средства создания и управления виртуальной инфраструктурой (гипервизор I типа, гипервизор II типа, гипервизор системы хранения данных, консоль управления виртуальной инфраструктурой и др.);

- виртуальные вычислительные системы (ВВС, виртуальные сервера и др.);

- виртуальные системы хранения данных;

- виртуальные каналы передачи данных;

- отдельные виртуальные устройства обработки, хранения и передачи данных (виртуальные процессоры, виртуальные диски, виртуальную память, виртуальное активное и пассивное сетевое оборудование и др.);

- виртуальные средства защиты информации (ЗИ) и средства ЗИ, предназначенные для использования в среде виртуализации;

- периметр виртуальной инфраструктуры (задействованные при реализации технологий виртуализации центральные процессоры и их ядра, адресное пространство памяти, сетевые интерфейсы, порты подключения внешних устройств и др.).

5.3. Для защиты перечисленных объектов используют как виртуальные средства ЗИ и средства ЗИ, предназначенные для использования в среде виртуализации, являющиеся разновидностями средств ЗИ, так и другие виды средств ЗИ.

5.4. Угрозы безопасности, обусловленные использованием технологий виртуализации.

5.4.1. Использование технологий виртуализации создает предпосылки для появления угроз

безопасности, не характерных для информационных систем, построенных без использования технологий виртуализации. Общий перечень угроз, дополнительно могущих возникать при использовании технологий виртуализации, включает угрозы, описанные далее.

5.4.2. Угрозы атаки на активное и/или пассивное виртуальное и/или физическое сетевое оборудование из физической и/или виртуальной сети.

5.4.3. Данные угрозы появляются в связи с ограниченностью функциональных возможностей (наличием слабостей) активного и/или пассивного виртуального и/или физического сетевого оборудования, входящего в состав виртуальной инфраструктуры. На реализацию данных угроз прямое влияние оказывают: наличие уязвимостей программного и/или микропрограммного обеспечения указанного оборудования, наличие у него фиксированного сетевого адреса и другие параметры его настройки, возможность изменения алгоритма работы программного обеспечения (ПО) сетевого оборудования вредоносными программами.

5.4.4. Угрозы атаки на виртуальные каналы передачи. Данные угрозы связаны со слабостями технологий виртуализации, с помощью которых строят виртуальные каналы передачи данных (сетевых технологий виртуализации). Некорректное использование сетевых технологий виртуализации может обеспечивать возможность несанкционированного перехвата трафика сетевых узлов, недоступных с помощью других сетевых технологий.

5.5. Угрозы атаки на гипервизор из виртуальной машины и/или физической сети.

5.5.1. Слабость гипервизора, а также слабость программных средств и ограниченность функциональных возможностей аппаратных средств, используемых для обеспечения его работоспособности. Реализация данных угроз приводит к недоступности всей (если гипервизор один) или части (если используют несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры.

5.5.2. Наличие у гипервизоров сетевых программных интерфейсов, предназначенных для удаленного управления составом и конфигурацией виртуальных устройств, созданных (создаваемых) данными гипервизорами, что позволяет злоумышленнику удаленно осуществлять несанкционированный доступ (НСД) к этим устройствам с помощью сетевых технологий из виртуальной и/или физической сети. Возможный ущерб может быть связан с доступностью данных виртуальных устройств.

5.5.3. Наличие у создаваемых ВВС сетевых адресов и возможность осуществления ими сетевого взаимодействия с другими субъектами как с помощью стандартных сетевых технологий, так и с помощью сетевых технологий виртуализации.

5.5.4. Атака на систему хранения данных из виртуальной и/или физической сети. Угрозы данного типа реализуются за счет слабостей применяемых технологий распределения информации по различным виртуальным устройствам хранения данных и/или виртуальным дискам, а также слабостей технологии единого виртуального дискового пространства. Указанные слабости связаны со сложностью алгоритмов обеспечения согласованности при реализации процессов распределения информации в рамках единого виртуального дискового пространства, а также взаимодействия с виртуальными и физическими каналами передачи данных для обеспечения работы в рамках одного дискового пространства.

5.5.5. Выход процесса за пределы виртуальной машины. Данная угроза связана с наличием слабостей ПО гипервизора, реализующего функцию изолированной программной среды для функционирующих в ней программ. В случае запуска вредоносной программой собственного гипервизора, функционирующего по уровню логического взаимодействия ниже компрометируемого гипервизора, последний, как и запущенные в нем средства защиты, не способен выполнять функции безопасности в отношении программ, функционирующих в собственном гипервизоре.

5.5.6. Несанкционированный доступ к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение. Данная угроза связана с наличием слабостей ПО гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения программного кода не только защищаемой информации и обрабатывающих ее программ, но и программного кода, реализующего виртуальное аппаратное обеспечение (виртуальные устройства обработки, хранения и передачи данных), от НСД со стороны вредоносной программы, функционирующей внутри ВВС. В случае осуществления НСД со стороны вредоносной программы, функционирующей внутри ВВС, к данным, хранящимся за пределами зарезервированного под пользовательские данные адресного пространства данной ВВС, вредоносная программа может не только нарушать целостность программного кода своей и/или других ВВС, функционирующих под управлением того же гипервизора, но и изменять параметры его (их) настройки.

5.5.7. Нарушение изоляции пользовательских данных внутри виртуальной машины. Данная угроза связана с наличием слабостей ПО гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения пользовательских данных программ, функционирующих внутри ВВС, от НСД со стороны вредоносного ПО, функционирующего вне ВВС. В результате реализации данной угрозы может быть нарушена безопасность пользовательских данных программ, функционирующих внутри ВВС.

5.5.8. Нарушение процедуры аутентификации субъектов виртуального информационного взаимодействия. Данная угроза связана с наличием множества различных протоколов взаимной идентификации и аутентификации виртуальных, виртуализованных и физических субъектов доступа, взаимодействующих между собой в ходе передачи данных как внутри одного уровня виртуальной инфраструктуры, так и между ее уровнями. Реализуемость данной угрозы напрямую зависит от качества реализации как самих протоколов, так и механизмов их взаимодействия.

5.5.9. Перехват управления гипервизором. Угроза перехвата управления гипервизором связана с наличием у консоли управления гипервизором программных интерфейсов взаимодействия с другими субъектами доступа (процессами, программами) и, как следствие, с возможностью НСД к данной консоли. Возможный ущерб может быть связан с нарушением безопасности информационных, программных и вычислительных ресурсов, зарезервированных и управляемых гипервизором.

5.5.10. Перехват управления средой виртуализации. Угроза перехвата управления средой виртуализации связаны с наличием у консоли управления виртуальной инфраструктурой, реализуемой в рамках одной из ВВС, а также у управляемых с ее помощью гипервизоров программных интерфейсов взаимодействия с другими программами и, как следствие, с возможностью НСД к указанному ПО уровня управления. Возможный ущерб может быть связан с нарушением безопасности информационных, программных и вычислительных ресурсов виртуальной инфраструктуры.

5.5.11. Неконтролируемый рост числа виртуальных машин. Данная угроза связана с наличием ограниченности объема дискового пространства, выделенного под виртуальную инфраструктуру и слабостями технологий контроля процесса создания ВВС, в связи с чем возможно случайное или несанкционированное преднамеренное создание множества ВВС. В результате реализации данной угрозы может быть ограничена или нарушена доступность виртуальных ресурсов для конечных пользователей облачных услуг.

5.5.12. Неконтролируемый рост числа зарезервированных вычислительных ресурсов. Данная угроза связана со слабостями ПО уровня управления виртуальной инфраструктурой, обеспечивающего выделение компьютерных ресурсов (вычислительных ресурсов и ресурсов памяти). Реализация данной угрозы возможна за счет НСД к указанному ПО и из-за ошибок в его коде.

5.5.13. Нарушение технологии обработки информации путем несанкционированного внесения изменений в образы виртуальных машин. Данная угроза связана с отсутствием в ПО

виртуализации защитных механизмов, предотвращающих НСД к образам ВВС. В результате реализации данной угрозы может быть нарушена конфиденциальность обрабатываемой с помощью данных ВВС защищаемой информации, целостность программ, установленных на ВВС, а также доступность ресурсов данных ВВС.

5.5.14. Несанкционированный доступ к хранимой в виртуальном пространстве защищаемой информации. В связи с применением множества технологий виртуализации, предназначенных для работы с данными (распределение данных внутри виртуальных и логических дисков, распределение данных между такими дисками, распределение данных между физическими и виртуальными накопителями единого дискового пространства, выделение областей дискового пространства в виде отдельных дисков и др.), практически все файлы хранятся в виде множества отдельных сегментов. Следовательно, в подавляющем большинстве случаев последовательное чтение данных с отдельно взятого носителя не позволяет нарушать конфиденциальность защищаемой информации, хранимой в системах хранения данных. В связи с этим меры по обеспечению конфиденциальности информации, хранящейся на отдельных накопителях, практически не применяют.

5.5.15. Ошибки обновления гипервизора. Данная угроза связана с зависимостью функционирования каждого виртуального устройства и каждого виртуализированного субъекта доступа, а также всей виртуальной инфраструктуры (или ее части, если используют более одного гипервизора) от работоспособности гипервизора. Некорректно обновленный гипервизор может привести к дискредитации функционирующих на его основе защитных механизмов, предотвращающих НСД к образам ВВС. Возможный ущерб может быть связан с нарушением конфиденциальности обрабатываемой с помощью данных ВВС защищаемой информации, целостности программ и доступности ресурсов данных ВВС.

Примечание. Ошибками обновления гипервизора являются:

- сбои в процессе его обновления;

- обновления, в ходе которых внедряются новые ошибки в код гипервизора;

- обновления, в ходе которых в гипервизор внедряется программный код, вызывающий несовместимость гипервизора со средой его функционирования;

- другие инциденты безопасности информации, происходящие в процессе обновления гипервизора.

5.6. Особенности защиты информации при использовании технологий виртуализации.

5.6.1. Защита информации, обрабатываемой в информационной системе (ИС), построенных с использованием технологий виртуализации, обеспечивается выполнением требований к мерам ЗИ. В целом меры ЗИ аналогичны мерам, применяемым в ИС, не использующих технологию виртуализации. Далее приведены специфические меры ЗИ, дополнительно применяемые при использовании технологий виртуализации.

5.6.2. Меры ЗИ разделены на несколько групп в зависимости от объекта защиты.

5.6.3. Меры ЗИ следует выбирать с учетом угроз безопасности, особенностей использования объектов защиты и действующего законодательства в области ЗИ.

5.6.4. Мерами защиты средств создания и управления виртуальной инфраструктурой являются:

- автоматическое изменение маршрутов передачи сетевых пакетов между компонентами виртуальной инфраструктуры внутри гипервизора;

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не

прошедших процедуру аутентификации;

- выявление, анализ и блокирование внутри виртуальной инфраструктуры скрытых каналов передачи информации в обход реализованных мер ЗИ или внутри разрешенных сетевых протоколов;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к консолям управления параметрами аппаратного обеспечения;

- контроль ввода (вывода) информации в/из виртуальную(ой) инфраструктуру(ы);

- контроль ввода (вывода) информации в/из ИС;

- контроль доступа субъектов доступа к изолированному адресному пространству в памяти гипервизора;

- контроль доступа субъектов доступа к изолированному адресному пространству в памяти хостовой операционной системы;

- контроль доступа субъектов доступа к средствам конфигурирования виртуального аппаратного обеспечения;

- контроль доступа субъектов доступа к средствам конфигурирования гипервизора и ВВС;

- контроль доступа субъектов доступа к средствам конфигурирования хостовой и/или гостевых операционных систем;

- контроль запуска гипервизора и ВВС на основе заданных критериев обеспечения безопасности объектов защиты (режим запуска, тип используемого носителя и т.д.);

- контроль запуска хостовой и/или гостевых операционных систем на основе заданных критериев обеспечения безопасности объектов защиты (режим запуска, тип используемого носителя и т.д.);

- контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях хостовой операционной системы, по следующим характеристикам: составу, объему и др.;

- контроль работоспособности дублирующих ключевых компонентов аппаратного обеспечения ИС;

- контроль работоспособности дублирующих ключевых компонентов виртуальной инфраструктуры;

- контроль целостности компонентов, критически важных для функционирования гипервизора и ВВС;

- контроль целостности компонентов, критически важных для функционирования хостовой и гостевых операционных систем;

- контроль целостности микропрограммного обеспечения аппаратной части ИС;

- мониторинг загрузки мощностей физического и виртуального аппаратного обеспечения;

- обеспечение возможности наследования установленных на уровне управления прав доступа субъектов доступа к объектам доступа на уровне виртуализации и оборудования;

- обеспечение изоляции различных потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры хостовой операционной системы;

- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

- отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры хостовой операционной системы;

- предотвращение задержки или прерывания выполнения в виртуальной инфраструктуре процессов с высоким приоритетом со стороны процессов с низким приоритетом;

- предотвращение задержки или прерывания выполнения процессов ВВС с высоким приоритетом со стороны процессов ВВС с низким приоритетом;

- применение индивидуальных прав доступа к объектам доступа субъектов доступа для одного или совокупности компонентов виртуальной инфраструктуры;

- проверка наличия вредоносных программ в загрузочных областях машинных носителей информации, подключенных к ИС;

- проверка наличия вредоносных программ в микропрограммном обеспечении физического и виртуального аппаратного обеспечения;

- проверка наличия вредоносных программ в файлах конфигурации гипервизора и/или ВВС;

- проверка наличия вредоносных программ в файлах конфигурации хостовой и гостевых операционных системах;

- проверка наличия вредоносных программ в файлах-образах виртуализованного ПО и ВВС, а также файлах-образах, используемых для обеспечения работы виртуальных файловых систем;

- проверка оперативной памяти и файловой системы гипервизора и/или ВВС на наличие вредоносных программ;

- проверка оперативной памяти и файловой системы хостовой и/или гостевых операционных систем на наличие вредоносных программ;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в виртуальном аппаратном обеспечении;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в гипервизоре и/или ВВС;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в хостовой и/или гостевых операционных системах;

- регистрация и учет запуска (завершения) работы компонентов виртуальной инфраструктуры;

- регистрация входа (выхода) субъектов доступа в/из гипервизор(а) и/или ВВС;

- регистрация входа (выхода) субъектов доступа в/из хостовую(ой) и/или гостевых операционных систем;

- регистрация запуска (завершения работы) гипервизора и/или ВВС, программ и процессов в гипервизоре и/или ВВС;

- регистрация запуска (завершения работы) хостовой и/или гостевых операционных систем, программ и процессов в хостовой и/или гостевых операционных системах;

- регистрация и учет изменений в составе программной и аппаратной части ИС во время ее функционирования и/или в период ее аппаратного отключения;

- регистрация изменений правил доступа к виртуальному аппаратному обеспечению;

- регистрация изменений состава и конфигурации виртуального аппаратного обеспечения;

- регистрация изменений состава и конфигурации ВВС;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в гипервизоре и/или ВВС;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в хостовой и/или гостевых операционных системах;

- регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в гипервизоре и/или ВВС;

- регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в хостовой и/или гостевых операционных системах;

- резервирование пропускной способности канала связи для обеспечения стабильного взаимодействия между компонентами виртуальной инфраструктуры внутри гипервизора;

- резервное копирование защищаемой информации в гипервизоре и/или ВВС, хранимой на физических и/или виртуальных носителях информации;

- резервное копирование защищаемой информации в хостовой и/или гостевых операционных системах, хранимой на физических и/или виртуальных носителях информации;

- резервное копирование физического и/или виртуального дискового пространства, используемого для хранения журналов событий гипервизора и/или ВВС;

- своевременное обнаружение отказов компонентов виртуальной инфраструктуры;

- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;

- стирание остаточной информации, образующейся после удаления данных, обрабатываемых в виртуальной инфраструктуре, содержащих информацию ограниченного доступа;

- стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в гипервизоре и/или ВВС;

- стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в хостовой и/или гостевых операционных системах;

- стирание остаточной информации, образующейся после удаления файлов, содержащих настройки виртуализованного ПО и виртуального аппаратного обеспечения;

- управление доступом к аппаратному обеспечению ИС, контроль подключения (отключения) машинных носителей информации;

- управление запуском (обращениями) компонентов ПО, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов ПО;

- управление установкой (инсталляцией) компонентов ПО, входящего в состав виртуальной инфраструктуры, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов ПО;

- установка (инсталляция) только разрешенного к использованию в виртуальной инфраструктуре ПО и/или его компонентов;

- фильтрация сетевого трафика между компонентами виртуальной инфраструктуры и внешними сетями хостовой операционной системы, в том числе сетями общего пользования;

- фильтрация сетевого трафика от/к каждой гостевой операционной системы(е).

5.6.5. Мерами защиты виртуальных вычислительных систем являются:

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- контроль доступа субъектов доступа к изолированному адресному пространству в памяти гипервизора;

- контроль доступа субъектов доступа к изолированному адресному пространству в памяти хостовой операционной системы;

- контроль доступа субъектов доступа к средствам конфигурирования гипервизора и ВВС;

- контроль доступа субъектов доступа к средствам конфигурирования хостовой и/или гостевых операционных систем;

- контроль доступа субъектов доступа к файлам-образам виртуализованного ПО и ВВС, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- контроль запуска гипервизора и ВВС на основе заданных критериев обеспечения безопасности объектов защиты (режима запуска, типа используемого носителя и т.д.);

- контроль запуска хостовой и/или гостевых операционных систем на основе заданных критериев обеспечения безопасности объектов защиты (режима запуска, типа используемого носителя и т.д.);

- контроль целостности компонентов, критически важных для функционирования гипервизора и ВВС;

- контроль целостности компонентов, критически важных для функционирования хостовой и гостевых операционных систем;

- контроль целостности файлов, содержащих настройки виртуализованного ПО и ВВС;

- контроль целостности файлов-образов виртуализованного ПО и ВВС, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

- предотвращение задержки или прерывания выполнения процессов ВВС с высоким приоритетом со стороны процессов ВВС с низким приоритетом;

- проверка наличия вредоносных программ в микропрограммном обеспечении физического и виртуального аппаратного обеспечения;

- проверка наличия вредоносных программ в файлах конфигурации гипервизора и/или ВВС;

- проверка наличия вредоносных программ в файлах конфигурации хостовой и гостевых операционных системах;

- проверка наличия вредоносных программ в файлах-образах виртуализованного ПО и ВВС, а также файлах-образах, используемых для обеспечения работы виртуальных файловых систем;

- проверка оперативной памяти и файловой системы гипервизора и/или ВВС на наличие вредоносных программ;

- проверка оперативной памяти и файловой системы хостовой и/или гостевых операционных систем на наличие вредоносных программ;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в виртуальном аппаратном обеспечении;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в гипервизоре и/или ВВС;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в хостовой и/или гостевых операционных системах;

- регистрация входа (выхода) субъектов доступа в/из гипервизор(а) и/или ВВС;

- регистрация входа (выхода) субъектов доступа в/из хостовой и/или гостевых операционных системах (систем);

- регистрация запуска (завершения работы) гипервизора и/или ВВС, программ и процессов в гипервизоре и/или ВВС;

- регистрация запуска (завершения работы) хостовой и/или гостевых операционных систем, программ и процессов в хостовой и/или гостевых операционных системах;

- регистрация изменений прав доступа к файлам-образам виртуализованного ПО и ВВС, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- регистрация изменений правил доступа к виртуальному аппаратному обеспечению;

- регистрация изменений состава и конфигурации ВВС;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в гипервизоре и/или ВВС;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в хостовой и/или гостевых операционных системах;

- регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в гипервизоре и/или ВВС;

- регистрация изменения правил доступа к информации ограниченного доступа, хранимой и обрабатываемой в хостовой и/или гостевых операционных системах;

- резервное копирование защищаемой информации в гипервизоре и/или ВВС, хранимой на физических и/или виртуальных носителях информации;

- резервное копирование защищаемой информации в хостовой и/или гостевых операционных системах, хранимой на физических и/или виртуальных носителях информации;

- резервное копирование файлов-образов виртуализованного ПО и ВВС, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

- резервное копирование физического и/или виртуального дискового пространства, используемого для хранения журналов событий гипервизора и/или ВВС;

- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;

- стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в гипервизоре и/или ВВС;

- стирание остаточной информации, образующейся после удаления данных, содержащих информацию ограниченного доступа, в хостовой и/или гостевых операционных системах;

- стирание остаточной информации, образующейся после удаления файлов-образов ВВС, в которых обрабатывалась информация ограниченного доступа;

- установка (инсталляция) только разрешенного к использованию в виртуальной инфраструктуре ПО и/или его компонентов;

- фильтрация сетевого трафика от/к каждой гостевой операционной системы(е);

- шифрование файлов-образов виртуализованного ПО и ВВС, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем, содержащих информацию ограниченного доступа.

5.6.6. Мерами защиты виртуальных систем хранения данных являются:

- автоматическое восстановление работоспособности системы хранения данных, подключенной к виртуальной инфраструктуре, в случае отказа одного или нескольких ее компонентов;

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- контроль ввода (вывода) информации в/из систему(ы) хранения данных, входящей в состав

виртуальной инфраструктуры;

- контроль доступа субъектов доступа к средствам конфигурирования системы хранения данных, входящей в состав виртуальной инфраструктуры;

- контроль доступа субъектов доступа к файлам-образам виртуализованного ПО и ВВС, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- контроль работоспособности (изношенности) машинных носителей информации, подключенных к виртуальной инфраструктуре, переход на дублирующие при необходимости;

- контроль целостности данных, хранимых на машинных носителях информации, подключенных к виртуальной инфраструктуре;

- контроль целостности файлов-образов виртуализованного ПО и ВВС, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

- обеспечение доверенных (защищенных) канала, маршрута передачи данных в/из систему(ы) хранения данных, входящую(ей) в состав виртуальной инфраструктуры;

- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

- проверка наличия вредоносных программ в операционной среде гипервизора системы хранения данных;

- проверка наличия вредоносных программ в файлах-образах виртуализованного ПО и ВВС, а также файлах-образах, используемых для обеспечения работы виртуальных файловых систем;

- разделение данных в зависимости от уровня конфиденциальности обрабатываемой информации между компонентами системы хранения данных, отдельными машинными носителями информации, входящими в состав виртуальной инфраструктуры, логическими дисками или между папками файлов;

- размещение системы хранения данных в защищенном сегменте информационной системы;

- регистрация изменений прав доступа к информации, хранящейся в системе хранения данных, входящей в состав виртуальной инфраструктуры;

- регистрация изменений прав доступа к файлам-образам виртуализованного ПО и ВВС, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- регистрация изменений правил доступа к виртуальному и физическому аппаратному обеспечению системы хранения данных;

- регистрация изменений состава и конфигурации виртуального и физического аппаратного обеспечения системы хранения данных;

- резервное копирование файлов-образов виртуализованного ПО и ВВС, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;

- управление доступом к аппаратному обеспечению системы хранения данных, контроль подключения (отключения) машинных носителей информации к/от виртуальной инфраструктуре(ы);

- шифрование файлов-образов виртуализованного ПО и ВВС, а также файлов-образов, используемых для обеспечения работы виртуальных файловых систем, содержащих информацию ограниченного доступа.

5.6.7. Мерами защиты виртуальных каналов передачи данных являются:

- автоматическое восстановление работоспособности системы хранения данных, подключенной к виртуальной инфраструктуре, в случае отказа одного или нескольких ее компонентов;

- автоматическое изменение маршрутов передачи сетевых пакетов между компонентами виртуальной инфраструктуры внутри гипервизора;

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- выявление, анализ и блокирование внутри виртуальной инфраструктуры скрытых каналов передачи информации в обход реализованных мер ЗИ или внутри разрешенных сетевых протоколов;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях хостовой операционной системы, по следующим характеристикам: составу, объему и др.;

- мониторинг загрузки мощностей физического и виртуального аппаратного обеспечения;

- обеспечение изоляции различных потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры хостовой операционной системы;

- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

- отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры хостовой операционной системы;

- передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией ограниченного доступа, обрабатываемой в виртуальной инфраструктуре, при обмене информацией с иными ИС;

- резервирование пропускной способности канала связи для обеспечения стабильного взаимодействия между компонентами виртуальной инфраструктуры внутри гипервизора;

- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;

- фильтрация сетевого трафика между компонентами виртуальной инфраструктуры и внешними сетями хостовой операционной системы, в том числе сетями общего пользования;

- фильтрация сетевого трафика от/к каждой гостевой операционной системы(е);

- шифрование информации ограниченного доступа, передаваемой по виртуальным и физическим каналам связи гипервизора;

- шифрование информации ограниченного доступа, передаваемой по виртуальным и физическим каналам связи хостовой операционной системы.

5.6.8. Мерами защиты виртуальных устройств обработки, хранения и передачи данных являются:

- блокировка доступа к объектам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- контроль доступа субъектов доступа к средствам конфигурирования виртуального аппаратного обеспечения;

- контроль доступа субъектов доступа к файлам-образам виртуализованного ПО и ВВС, а также файлам-образам, используемым для обеспечения работы виртуальных файловых систем;

- контроль работоспособности дублирующих ключевых компонентов виртуальной инфраструктуры;

- контроль целостности файлов, содержащих настройки виртуализованного ПО и ВВС;

- мониторинг загрузки мощностей физического и виртуального аппаратного обеспечения;

- обеспечение возможности наследования установленных на уровне управления прав доступа субъектов доступа к объектам доступа на уровни виртуализации и оборудования;

- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

- отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры хостовой операционной системы;

- применение индивидуальных прав доступа к объектам доступа субъектов доступа для одного или совокупности компонентов виртуальной инфраструктуры;

- проверка наличия вредоносных программ в микропрограммном обеспечении физического и виртуального аппаратного обеспечения;

- разделение физических ресурсов между компонентами виртуальной инфраструктуры в зависимости от уровня конфиденциальности обрабатываемой информации;

- размещение сенсоров и/или датчиков систем обнаружения (предотвращения) вторжений в виртуальном аппаратном обеспечении;

- регистрация и учет запуска (завершения) работы компонентов виртуальной инфраструктуры;

- регистрация и учет изменений в составе программной и аппаратной части ИС во время ее

функционирования и/или в период ее аппаратного отключения;

- регистрация изменений правил доступа к виртуальному аппаратному обеспечению;

- регистрация изменений состава и конфигурации виртуального аппаратного обеспечения;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в гипервизоре и/или BBC;

- регистрация изменений состава ПО и виртуального аппаратного обеспечения в хостовой и/или гостевых операционных системах;

- резервное копирование защищаемой информации, хранимой на физических и виртуальных носителях информации;

- своевременное обнаружение отказов компонентов виртуальной инфраструктуры;

- создание (имитация) ложных компонентов виртуальной инфраструктуры, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности;

- стирание остаточной информации, образующейся после удаления файлов, содержащих настройки виртуализованного ПО и виртуального аппаратного обеспечения;

- управление доступом к аппаратному обеспечению ИС, контроль подключения (отключения) машинных носителей информации.

5.6.9. Мерами защиты виртуальных средств защиты информации и средств защиты информации, предназначенных для использования в среде виртуализации, являются:

- автоматическое восстановление всех функций средств ЗИ, входящих в состав ИС;

- защита от НСД к вводимой субъектами доступа, входящими в состав виртуальной инфраструктуры, аутентификационной информации;

- защита от НСД к хранящейся в компонентах виртуальной инфраструктуры аутентификационной информации о субъектах доступа;

- идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении к объектам виртуальной инфраструктуры;

- обеспечение возможности наследования установленных на уровне управления прав доступа субъектов доступа к объектам доступа на уровни виртуализации и оборудования;

- обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами ЗИ (функциями безопасности средств ЗИ).

VI. МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Для эффективной реакции на инциденты ИБ Служба:

- разрабатывает и документирует политику менеджмента инцидентов ИБ, а также получает очевидную поддержку этой политики заинтересованными сторонами и, в особенности, высшего руководства;

- разрабатывает и в полном объеме документирует систему менеджмента инцидентов ИБ для поддержки политики менеджмента инцидентов ИБ. Формы, процедуры и инструменты поддержки обнаружения, оповещения, оценки и реагирования на инциденты ИБ, а также градации шкалы серьезности инцидентов отражаются в документации на конкретную систему - План реагирования

на инциденты ИБ;

- обновляет политику менеджмента ИБ и рисков на всех уровнях, то есть на корпоративном и для каждой системы, сервиса и сети отдельно с учетом системы менеджмента инцидентов ИБ;

- создает в Организации соответствующее структурное подразделение менеджмента инцидентов ИБ, то есть ГРИИБ, с заданными обязанностями и ответственностью персонала, способного адекватно реагировать на все известные типы инцидентов ИБ. В большинстве организаций ГРИИБ является группой, состоящей из специалистов по конкретным направлениям деятельности, например, при отражении атак вредоносной программы привлекают специалиста по инцидентам подобного типа;

- знакомит весь персонал Организации посредством инструктажей и (или) иными способами с существованием системы менеджмента инцидентов ИБ, ее преимуществами и с надлежащими способами сообщения о событиях ИБ. Проводит соответствующее обучение персонала, ответственного за управление системой менеджмента инцидентов ИБ, лиц, принимающих решения по определению того, являются ли события инцидентами, и лиц, исследующих инциденты;

- тестирует систему менеджмента инцидентов ИБ.

6.2. Применение системы менеджмента инцидентов информационной безопасности включает:

- обнаружение и оповещение о возникновении событий ИБ (человеком или автоматическими средствами);

- сбор информации, связанной с событиями ИБ, и оценка этой информации с целью определения, какие события можно отнести к категории инцидентов ИБ;

- реагирование на инциденты ИБ:

- исключение несанкционированного доступа к информационным ресурсам;

- администрирование защиты (безопасности) информационных ресурсов;

- создание и выдача пользователям ИС ключей шифрования информации;

- проведение аттестационных испытаний объектов информатизации, обрабатывающих конфиденциальную информацию Организации;

- участие в подготовке организационно-распорядительных документов по обеспечению защиты информации;

- разграничение доступа к информационным ресурсам;

- проведение технического обслуживания и ремонт средств вычислительной техники, обрабатывающей информацию ограниченного доступа, с учетом требований по защите информации;

- немедленное реагирование на инциденты ИС;

- если инциденты ИБ находятся под контролем, выполнение менее срочных действий (например, способствующих полному восстановлению после катастрофы);

- если инциденты ИБ не находятся под контролем, выполнение "антикризисных" действий (например, вызов пожарной команды/аварийной службы/подразделения безопасности или инициирование выполнения плана непрерывности бизнеса);

- сообщить о наличии инцидентов ИБ и любые относящиеся к ним подробности персоналу Организации, а также персоналу сторонних организаций (что может включить в себя, по мере необходимости, распространение подробностей инцидента с целью дальнейшей оценки и (или) принятия решений);

- правовую экспертизу;

- надлежащую регистрацию всех действий и решений для последующего анализа;

- разрешение проблемы инцидентов.

6.3. После разрешения/закрытия инцидентов ИБ Служба организует осуществление следующих действий по анализу состояния ИБ:

- проведение дополнительной правовой экспертизы (при необходимости);

- изучение уроков, извлеченных из инцидентов ИБ;

- определение улучшений для внедрения защитных мер ИБ, полученных из уроков, извлеченных из одного или нескольких инцидентов ИБ;

- определение улучшений для системы менеджмента инцидентов ИБ в целом, учитывая уроки, извлеченные из результатов анализа качества предпринимаемого подхода (например, из анализа результативности процессов, процедур, форм отчета и (или) организации).

6.4. Процессы менеджмента инцидентов ИБ являются итеративными, с постоянным внесением улучшений с течением времени в ряд элементов ИБ. Эти улучшения предлагаются на основе данных об инцидентах ИБ и реагировании на них, а также данных о динамике тенденций. Этап "Улучшение" включает в себя:

- пересмотр имеющихся результатов анализа рисков ИБ и анализ менеджмента организации;

- улучшение системы менеджмента инцидентов ИБ и ее документации;

- инициирование улучшений в области безопасности, включая внедрение новых и (или) обновленных защитных мер ИБ.

6.5. Преимущества менеджмента объединяются в следующие группы:

6.5.1. Улучшение безопасности. Структурный процесс обнаружения, оповещения, оценки и менеджмента инцидентов и событий ИБ позволяет быстро идентифицировать любое событие или инцидент ИБ и реагировать на них, тем самым улучшая общую безопасность за счет быстрого определения и реализации правильного решения, а также обеспечивая средства предотвращения подобных инцидентов ИБ в будущем.

6.5.2. Снижение негативных воздействий на бизнес. Структурный подход к менеджменту инцидентов ИБ может способствовать снижению уровня негативных воздействий, связанных с инцидентами ИБ, на бизнес. Последствия этих воздействий могут включать в себя немедленные финансовые убытки, а также долговременные потери, возникающие от ущерба, нанесенного репутации и кредитоспособности организации.

6.5.3. Усиление внимания к предотвращению инцидентов. Использование структурного подхода к менеджменту инцидентов ИБ может способствовать усилению внимания к предотвращению инцидентов внутри организации. Анализ данных, связанных с инцидентами, позволяет определить модели и тенденции появления инцидентов, тем самым способствуя усилению внимания к предотвращению инцидентов и, следовательно, определению соответствующих действий по предотвращению возникновения инцидентов.

6.5.4. Усиление внимания к системе установления приоритетов и свидетельств. Структурный

подход к менеджменту инцидентов ИБ создает прочную основу для системы установления приоритетов при проведении расследований инцидентов ИБ.

6.5.5. Бюджет и ресурсы. Хорошо продуманный структурный подход к менеджменту инцидентов ИБ способствует обоснованию и упрощению распределения бюджетов и ресурсов внутри подразделений Организации. Выгоды самой системы менеджмента инцидентов ИБ:

- использование менее квалифицированного персонала для идентификации и фильтрации ложных сигналов тревоги;

- обеспечение лучшего руководства действиями квалифицированного персонала;

- привлечение квалифицированного персонала только для тех процессов, где требуются его навыки, и только на той стадии процесса, где его содействие необходимо.

6.5.6. Менеджмент и анализ рисков ИБ. Использование структурного подхода к менеджменту инцидентов ИБ способствует:

- сбору более качественных данных для идентификации и определения характеристик различных типов угроз и связанных с ними уязвимостей;

- предоставлению данных о частоте возникновения идентифицированных типов угроз.

Полученные данные о негативных последствиях инцидентов ИБ для бизнеса будут полезны для анализа этих последствий. Данные о частоте возникновения различных типов угроз намного повысят качество оценки угроз. Аналогично, данные об уязвимостях намного повысят качество будущих оценок уязвимостей.

Вышеупомянутые данные значительно улучшат результаты анализа менеджмента и анализа рисков ИБ.

6.5.7. Осведомленность в вопросах ИБ. Структурный подход к менеджменту инцидентов ИБ предоставляет узконаправленную информацию о программах обеспечения осведомленности в вопросах ИБ. Эта информация является источником реальных примеров, на которых можно показать, что инциденты ИБ действительно происходят именно в данной организации, а не где-либо еще. Таким образом можно продемонстрировать выгоды быстрого получения информации о решениях. Более того, подобная осведомленность в вопросах ИБ позволяет снизить вероятность ошибки, возникновения паники и (или) растерянности у людей в случае появления инцидента ИБ.

6.5.8. Входные данные для анализа политики ИБ. Информация, предоставляемая системой менеджмента инцидентов ИБ, может обеспечить ценные входные данные для анализа результативности и последующего улучшения политик ИБ (и другой документации, связанной с ИБ). Это относится к политикам и другой документации как на уровне организации, так и для отдельных систем, сервисов и сетей.

6.6. Обязательства руководства. Для принятия структурного подхода к менеджменту инцидентов ИБ жизненно необходима постоянная поддержка со стороны руководства. Персонал организации должен распознавать инциденты ИБ и знать свои действия при их возникновении, а также осознавать большие преимущества структурного подхода для организации. Однако этого может быть недостаточно при отсутствии поддержки со стороны руководства. Необходимо донести до руководства, что организация должна выполнять обязательства по обеспечению ресурсами и поддержке способности реагирования на инциденты.

6.7. Правовые и нормативные аспекты, в том числе:

- обеспечение адекватной защиты персональных данных и неприкосновенность персональной информации;

- лица, имеющие доступ к персональным данным, не должны лично знать тех людей, информация о которых изучается;

- лица с доступом к личным данным должны подписать соглашение об их неразглашении до того, как получат доступ к ним;

- персональные данные должны использоваться исключительно для тех целей, для которых они были получены, то есть для расследования инцидентов ИБ;

- соответствующее хранение записей;

- наличие защитных мер для обеспечения выполнения коммерческих договорных обязательств;

- правовые вопросы, связанные с политиками и процедурами;

- проверка на законность непризнания ответственности;

- включение в контракты со сторонним персоналом всех необходимых аспектов;

- соглашения о неразглашении конфиденциальной информации;

- исполнение требований правоприменяющих органов;

- ясность в вопросах ответственности;

- специальные нормативные требования;

- судебные преследования или внутренние дисциплинарные разбирательства. Для успешного судебного преследования или проведения дисциплинарных разбирательств внутри организации в отношении злоумышленников независимо от того, были ли эти атаки техническими или физическими, необходимо применять соответствующие меры защиты ИБ, включая доказуемо защищенные от внесения изменений журналы аудита. Для обеспечения успешного судебного преследования или проведения дисциплинарных разбирательств внутри организации в отношении злоумышленников независимо от того, были ли эти атаки техническими или физическими, необходимо собрать свидетельства для федеральных судов или других административных органов. Необходимо показать, что:

а) документация не подвергалась искажениям и является полной;

б) копии электронного свидетельства доказуемо идентичны оригиналам;

в) все системы ИТ, от которых были получены свидетельства, во время регистрации работали в штатном режиме;

- правовые аспекты, связанные с методами мониторинга;

- подготовка правил пользования информационными ресурсами и ознакомление с ними.

6.8. Эксплуатационная эффективность и качество. Эффективность эксплуатации и качество структурного подхода к менеджменту инцидентов ИБ зависит от ряда факторов, включающих в себя обязательность уведомления об инцидентах, качество уведомления, простоту использования, быстродействие и обучение. Некоторые из этих факторов связаны с обеспечением осведомленности пользователей о важности менеджмента инцидентов ИБ и их мотивированностью сообщать об инцидентах. Что касается быстродействия, то время, используемое на сообщение об инциденте ИБ, - не единственный фактор, важно также учитывать время, необходимое для обработки данных и распространения обработанной информации (особенно в случае с сигналами аварийности). Для минимизации задержек соответствующие программы обеспечения осведомленности и обучения пользователей должны дополняться

поддержкой по горячей линии, которая обеспечивается персоналом, осуществляющим менеджмент инцидентов ИБ.

6.9. Анонимность. Пользователи должны быть уверены, что информация об инцидентах ИБ, которую они сообщают, полностью защищена, а при необходимости обезличена, с тем чтобы ее невозможно было связать с их организацией или ее подразделением без их согласия. Система менеджмента инцидентов ИБ должна учитывать ситуации, когда важно обеспечить анонимность лица или организации, сообщающих о потенциальных инцидентах ИБ при особых обстоятельствах. У каждой организации должны быть положения, в которых четко разъяснялись бы важность сохранения анонимности или ее отсутствия для лиц и организаций, сообщающих о потенциальном инциденте ИБ. ГРИИБ может потребоваться дополнительная информация, не сообщенная изначально информирующим об инциденте лицом или организацией. Более того, важная информация об инциденте ИБ может быть получена от первого обнаружившего его лица.

6.10. Конфиденциальность. Во время обработки необходимо обеспечивать анонимность информации, или персонал должен подписать соглашение о конфиденциальности (неразглашении) при получении доступа к ней. Кроме того, система менеджмента инцидентов ИБ должна обеспечивать контроль за передачей сообщений об инцидентах сторонними организациями, включая СМИ, партнеров по бизнесу, потребителей, регулирующие организации и общественность.

6.11. Независимость деятельности ГРИИБ. Группа менеджмента инцидентов ИБ должна быть способна эффективно удовлетворять функциональные, финансовые, правовые и политические потребности конкретной организации и быть в состоянии соблюдать осторожность при управлении инцидентами ИБ. Деятельность группы менеджмента инцидентов ИБ должна также подвергаться независимому аудиту с целью проверки эффективности ее функционирования. Эффективным способом реализации независимости контроля является отделение цепочки сообщений о реагировании на инцидент ИБ от общего оперативного руководства и возложение на вышестоящего руководителя непосредственных обязанностей по управлению реагированием на инциденты. Финансирование работы группы, во избежание чрезмерного влияния на нее со стороны, также должно быть отдельным.

6.12. Политика менеджмента инцидентов информационной безопасности.

6.12.1. Назначение политики. Политика менеджмента инцидентов ИБ предназначена для всего персонала, имеющего авторизованный доступ к информационным системам организации и местам их расположения.

6.12.2. Лица, связанные с политикой менеджмента инцидентов информационной безопасности. Политика менеджмента инцидентов ИБ утверждается старшим должностным лицом организации с документально подтвержденными полномочиями, полученными от высшего руководства. Политика должна быть доступна для каждого сотрудника и подрядчика и доведена через инструктаж и обучение с целью обеспечения их осведомленности в области ИБ.

6.12.3. Содержание политики менеджмента инцидентов информационной безопасности.

Политика менеджмента инцидентов ИБ должна включать в себя следующие вопросы:

- значимость менеджмента инцидентов ИБ для организации, а также обязательства высшего руководства относительно поддержки менеджмента и его системы;

- общее представление об обнаружении событий ИБ, оповещении о них и сборе соответствующей информации, а также о путях использования этой информации для определения инцидентов ИБ. Это общее представление должно содержать перечень возможных событий ИБ, а также информацию о том, как сообщать о ней, что, где и кому сообщать, а также как обращаться с совершенно новыми событиями ИБ;

- общее представление об оценке инцидентов ИБ, включая перечень ответственных лиц,

необходимые для выполнения действия, уведомления об инцидентах и дальнейшие действия ответственных лиц;

- краткое изложение действий после подтверждения того, что событие ИБ является инцидентом ИБ. Эти действия представляют:

- немедленное реагирование;

- правовую экспертизу;

- передачу информации соответствующему персоналу или сторонним организациям;

- проверку, находится ли инцидент ИБ под контролем;

- дальнейшее реагирование;

- объявление "кризисной ситуации";

- определение критериев усиления реагирования на инциденты ИБ;

- определение ответственного за инцидент лица;

- ссылку на необходимость правильной регистрации всех действий для дальнейшего и непрерывного мониторинга с целью обеспечения защищенного хранения свидетельств в электронном виде на случай их востребования для судебного разбирательства или дисциплинарного расследования внутри организации;

- действия, следующие за разрешением инцидента ИБ, включая извлечение урока из инцидента и улучшение процесса, следующего за инцидентами ИБ;

- подробности места хранения документации о системе, включая процедуры хранения;

- общее представление о деятельности ГРИИБ, включающее в себя следующие вопросы:

организационную структуру ГРИИБ и весь основной персонал группы, включая лиц, ответственных:

- за краткое информирование высшего руководства об инцидентах;

- проведение расследований и другие действия персонала группы после объявления "кризисной ситуации";

- связь со сторонними организациями (при необходимости);

- положение о менеджменте ИБ, область деятельности ГРИИБ и полномочия, в рамках которых она будет ее осуществлять. Это положение должно включать в себя, как минимум, формулировку целевого назначения, определение области деятельности ГРИИБ и подробности об учредителе ГРИИБ и его полномочиях;

- формулировку целей ГРИИБ применительно к основной деятельности группы персонала. Для выполнения своих функций персонал должен участвовать в оценке инцидентов ИБ, реагировании на них и управлении ими, а также в их успешном разрешении. Для целей и назначения ГРИИБ требуется четкое и однозначное определение;

- определение сферы деятельности ГРИИБ. Обычно в сферу деятельности ГРИИБ организации входят все информационные системы, сервисы и сети организации. В некоторых случаях для организации может потребоваться сужение сферы действия ГРИИБ. При этом необходимо четко документировать, что входит и что не входит в сферу ее деятельности;

- личность учредителя ГРИИБ - старшего должностного лица (член правления, старший руководитель), который санкционирует действия ГРИИБ и устанавливает уровни полномочий, переданных ГРИИБ. Осведомленность об этом поможет всему персоналу организации понять предпосылки создания и структуру ГРИИБ, что является крайне важной информацией для формирования доверия к ГРИИБ. Следует отметить, что перед обнародованием подробностей о создании и структуре ГРИИБ необходимо проверить законность этого действия. В некоторых обстоятельствах раскрытие полномочий группы персонала может послужить причиной предъявления ей претензий по нарушению обязательств;

- общее представление о программе обеспечения осведомленности и обучения менеджменту инцидентов ИБ;

- перечень правовых и нормативных аспектов, предполагаемых к рассмотрению.

VII. СОЗДАНИЕ ГРУППЫ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Целью создания ГРИИБ является обеспечение организации соответствующим персоналом для оценки, реагирования на инциденты ИБ и извлечения уроков из них, а также необходимой координации, менеджмента, обратной связи и процесса передачи информации. Члены ГРИИБ могут участвовать в снижении физического и финансового ущерба, а также ущерба для репутации организации, связанного с инцидентами ИБ.

7.2. Состав и количество персонала, а также структура ГРИИБ должны соответствовать масштабу и структуре Организации. В организации ГРИИБ является отделом (или: внештатной группой, которая вправе привлекать сотрудников из различных подразделений Организации). ГРИИБ возглавляется одним из заместителей руководителя Организации.

7.3. Члены группы должны быть доступны для контакта так, чтобы их имена и имена лиц, их замещающих, а также подробности о контакте с ними были доступными внутри Организации. В документации системы менеджмента инцидентов ИБ должны быть четко указаны необходимые детали, включая любые документы по процедурам и формы отчетов, но не в положениях политики.

7.4. Руководитель ГРИИБ должен:

- иметь делегированные полномочия немедленного принятия решения о том, какие меры предпринять относительно инцидента;

- иметь отдельную линию для оповещения высшего руководства, которая должна быть изолирована от обычных бизнес-операций;

- обеспечивать необходимый уровень знаний и мастерства для всех членов ГРИИБ, а также поддержание этого уровня;

- поручать расследование каждого инцидента наиболее компетентному члену группы.

7.5. Руководитель ГРИИБ и члены группы обязаны и вправе предпринимать необходимые действия, адекватные инциденту ИБ. Действия, которые могут оказать неблагоприятное влияние на всю Организацию в отношении финансов или репутации, должны согласовываться с высшим руководством. О серьезных инцидентах ИБ руководитель ГРИИБ оповещает Главу Качканарского городского округа.

7.6. Процедуры общения со СМИ и ответственность за это общение также должны быть согласованы со старшим руководством, документированы и определять:

- представителя организации по работе со средствами массовой информации;

- метод взаимодействия подразделения организации с ГРИИБ.

7.7. Отношения со сторонними лицами и организациями.

7.7.1. К сторонним лицам и организациям относятся:

- сторонний вспомогательный персонал, работающий по контракту;

- ГРИИБ сторонних организаций;

- правоприменяющие организации;

- аварийные службы (например, пожарная бригада/отделение);

- соответствующие государственные организации;

- юридический персонал;

- официальные лица по связям с общественностью и (или) представителями средств массовой информации;

- партнеры по бизнесу;

- потребители;

- общественность.

7.7.2. Взаимодействие членов ГРИИБ со сторонними организациями и лицами допускается только по письменному распоряжению руководителя Организации.

7.8. Быстрое и эффективное реагирование на инциденты ИБ включает:

- получение, подготовку, тестирование технических и других средств поддержки и реагирования;

- доступ к актуальным деталям активов Организации и информацию по их связям с бизнес-функциями;

- доступ к документированной стратегии обеспечения непрерывности бизнеса и соответствующим планам;

- документированные и опубликованные процессы передачи информации;

- использование электронной базы данных событий/инцидентов ИБ и технических средств для быстрого пополнения и обновления базы данных, анализа ее информации и упрощения процессов реагирования (хотя общепризнано, что иногда сделанные вручную записи также оказываются востребованными и используются организацией);

- адекватные меры по обеспечению непрерывности бизнеса для базы данных событий/инцидентов ИБ.

VIII. ОБЕСПЕЧЕНИЕ ОСВЕДОМЛЕННОСТИ И ОБУЧЕНИЕ ПЕРСОНАЛА

8.1. Осведомленность и участие всего персонала Организации очень важны для обеспечения успеха менеджмента инцидентов ИБ. Программа обеспечения осведомленности и соответствующий материал должны быть доступны для всего персонала, включая новых служащих, пользователей сторонних организаций и подрядчиков.

8.1.1. Для группы обеспечения эксплуатации, для членов ГРИИБ, для персонала,

ответственного за ИБ, специальных администраторов разрабатываются специальные программы обучения.

8.1.2. Для каждой группы, непосредственно участвующей в менеджменте инцидентов, требуются различные уровни подготовки, зависящие от типа, частоты и значимости их взаимодействия с системой менеджмента инцидентов ИБ.

8.1.3. Инструктажи по обеспечению осведомленности должны включать в себя:

- основы работы системы менеджмента инцидентов ИБ, включая сферу ее действия и технологию работ по менеджменту инцидентов и событий ИБ;

- способы оповещения о событиях и инцидентах ИБ;

- защитные меры по обеспечению конфиденциальности источников (по необходимости);

- соглашения об уровнях сервиса системы;

- уведомление о результатах - на каких условиях будут информированы источники;

- любые ограничения, налагаемые соглашениями о неразглашении;

- полномочия организации менеджмента инцидентов ИБ и ее линия оповещения;

- кто и как получает отчеты от системы менеджмента инцидентов ИБ.

8.1.4. В программы ориентирования персонала или в общие корпоративные программы обеспечения осведомленности в вопросах ИБ включаются подробности обеспечения осведомленности о менеджменте инцидентов ИБ.

8.1.5. До ввода в эксплуатацию системы менеджмента инцидентов ИБ весь соответствующий персонал должен под роспись ознакомиться с процедурами обнаружения и оповещения о событиях ИБ.

8.1.6. Подготовка персонала должна сопровождаться специальными упражнениями и тестированием членов группы обеспечения эксплуатации и ГРИИБ, а также персонала, ответственного за ИБ, и специальных администраторов.

IX. ИСПОЛЬЗОВАНИЕ КСЗ

9.1. Использование КСЗ включает:

- обнаружение события ИБ и оповещение о нем одним из сотрудников персонала/клиентом организации или автоматически (например, сигналом тревоги от межсетевого экрана);

- сбор информации о событии ИБ и проведение первичной оценки персоналом группы обеспечения эксплуатации организации с целью определения, является ли событие инцидентом ИБ или ложным сигналом тревоги;

- проведение второй оценки ГРИИБ с целью подтвердить, что событие является инцидентом ИБ и, в положительном случае, инициировать немедленное реагирование, а также необходимость правовой экспертизы и действий по передаче информации;

- анализ, проводимый ГРИИБ с целью определить, находится ли инцидент под контролем:

- в положительном случае - инициация дальнейших мер реагирования и готовности всей системы для использования в процессе анализа последствий инцидента;

- при отрицательном ответе - инициация антикризисных действий с привлечением

соответствующего персонала, например руководителя и группы обеспечения непрерывности бизнеса организации;

- расширение области действия дальнейших оценок и (или) принятия решений, проводимое в течение всего этапа по требованию;

- обеспечение надлежащей регистрации всеми причастными лицами, в особенности членами ГРИИБ, всей деятельности для дальнейшего анализа;

- обеспечение сбора и защищенного хранения свидетельств в электронном виде и постоянного мониторинга защищенного хранения этих свидетельств на случай их востребованности для судебного преследования или внутреннего дисциплинарного разбирательства;

- поддержка режима контроля изменений, включая отслеживание инцидентов ИБ и обновления отчетов по инцидентам с тем, чтобы база данных событий/инцидентов ИБ постоянно соответствовала действительности.

9.2. Вся собранная информация, касающаяся событий или инцидентов ИБ, должна храниться в базе данных событий/инцидентов ИБ, управляемой ГРИИБ. Информация, сообщаемая в течение каждого процесса, должна быть как можно более полной в любое время, чтобы обеспечить наиболее прочную основу для оценок и принятия решений, а также для предпринимаемых действий.

9.3. После обнаружения события ИБ и сообщения о нем целями последующих процессов являются:

- распределение ответственности за деятельность, связанную с менеджментом инцидентов, через соответствующую иерархию персонала вместе с оценкой и принятием решений, а также за действия с привлечением персонала как связанного, так и не связанного с обеспечением безопасности;

- обеспечение формальных процедур для каждого оповещенного лица, включая анализ и корректировку сделанного сообщения, оценку ущерба и уведомление соответствующего персонала (действия каждого лица зависят от типа и опасности инцидента);

- использование рекомендаций для тщательного документирования событий ИБ, а позднее, если событие будет отнесено к инциденту ИБ, то и для последующих действий в отношении инцидента ИБ и обновления базы данных событий/инцидентов ИБ.

9.4. По обнаружению и оповещению о событиях ИБ, оценке и принятию решений (является ли событие инцидентом ИБ), реагированию на инциденты ИБ включают в себя:

- немедленное реагирование;

- анализ с целью определения, находится ли инцидент ИБ под контролем;

- последующие реагирования;

- антикризисные действия;

- правовую экспертизу;

- передачу информации;

- комментарий по вопросам расширения сферы менеджмента инцидентов ИБ;

- регистрацию деятельности.

9.5. События ИБ могут быть обнаружены непосредственно лицом или лицами, заметившими что-либо, вызывающее беспокойство и имеющее технический, физический или процедурный характер. Обнаружение может осуществляться, например, детекторами огня/дыма или с помощью охранной сигнализации путем передачи сигналов тревоги в заранее определенные места (для осуществления человеком определенных действий). Технические события ИБ могут обнаруживаться автоматически, например это могут быть сигналы тревоги, производимые устройствами анализа записей аудита, межсетевыми экранами, системами обнаружения вторжений, антивирусными программами, в каждом случае стимулируемые заранее установленными параметрами этих устройств.

9.5.1. Независимо от причины обнаружения события ИБ лицо, непосредственно обратившее внимание на нечто необычное или оповещенное автоматическими средствами, несет ответственность за инициирование процесса обнаружения и оповещения. Этим лицом может быть любой представитель персонала организации, работающий постоянно или по контракту. Этот представитель должен следовать процедурам и использовать форму отчета о событиях ИБ, определенную системой менеджмента инцидентов ИБ, с целью привлечения внимания прежде всего группы обеспечения эксплуатации и менеджмента. Следовательно, важно, чтобы весь персонал был ознакомлен с рекомендациями, относящимися к вопросу оповещения о возможных событиях ИБ, включая формы отчета, имел доступ к ним и знал сотрудников, которых необходимо оповещать о каждом случае появления события ИБ. Необходимо, чтобы весь персонал организации был по крайней мере осведомлен о форме отчета, что способствовало бы его пониманию системы менеджмента инцидентов ИБ.

9.5.2. Обработка конкретного события ИБ зависит от того, что оно собой представляет, а также от последствий и воздействий, к которым это событие может привести. Сотрудник, информирующий о событии ИБ, должен заполнить форму отчета так, чтобы в ней было как можно больше информации, доступной ему на тот момент. При необходимости он связывается со своим руководителем.

9.5.3. При заполнении формы отчета важна не только точность содержания, но и своевременность заполнения. Не следует задерживать представление формы отчета о событии ИБ по причине уточнения ее содержания.

9.5.4. При наличии проблем или при существовании мнения о наличии проблем с установленными по умолчанию механизмами электронного оповещения (например, электронной почтой), включая случаи атаки на систему и считывание формы отчета несанкционированными лицами, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть нарочные, телефон, текстовые сообщения. Такие альтернативные средства должны использоваться на ранних стадиях расследования, когда становится очевидным, что событие ИБ будет переведено в категорию инцидента ИБ, особенно такого инцидента ИБ, который может считаться значительным.

9.6. Оценка и принятие решений по событиям/инцидентам.

9.6.1. Первая оценка и предварительное решение. В группе обеспечения эксплуатации системы менеджмента инцидентов ИБ принимающее лицо должно подтвердить получение заполненной формы отчета, ввести ее в базу данных событий/инцидентов ИБ и проанализировать данную форму отчета. Далее должностное лицо должно попытаться получить любые уточнения от сообщившего лица о событии ИБ и собрать требуемую дополнительную информацию, считающуюся доступной, как от сообщившего о событии лица, так и из любого другого места. Затем представитель группы обеспечения эксплуатации должен провести оценку для определения, подходит ли это событие под категорию инцидента ИБ или является ложным. Если событие ИБ определяется как ложное, необходимо заполнить форму отчета и передать в ГРИИБ для записи в базу данных и дальнейшего анализа, а также создать копии для сообщившего о событии лица и его/ее местного руководителя.

9.6.1.1. Информация и другие свидетельства, собранные на этом этапе, могут потребоваться в

будущем для дисциплинарного или судебного разбирательства. Лицо или лица, выполняющие задачи сбора и оценки информации, должны хорошо знать требования по сбору и сохранению свидетельств.

9.6.1.2. Дополнительно к дате (датам) и времени выполнения действий необходимо полностью документировать:

- проведенные мероприятия (включая использованные средства) и их цели;

- место хранения свидетельства наличия события;

- способ архивирования свидетельства (если оно уместно);

- способ верификации свидетельства (если оно уместно);

- детали хранения материалов и последующего доступа к ним.

9.6.1.3. Если событие ИБ определено как вероятный инцидент ИБ, а сотрудник группы обеспечения эксплуатации имеет соответствующий уровень компетентности, то проводится дальнейшая оценка. В результате могут потребоваться корректирующие действия, например идентификация дополнительных "аварийных" защитных мер и обращение за помощью в их реализации к соответствующему лицу. Событие ИБ может быть определено как инцидент ИБ, причем значительный (по шкале серьезности, принятой в организации), в этом случае необходимо проинформировать непосредственно руководителя ГРИИБ. Может потребоваться объявление "кризисной ситуации" и, как следствие, уведомление руководителя обеспечения непрерывности бизнеса о возможной активизации плана обеспечения непрерывности бизнеса с одновременным информированием руководителя ГРИИБ и вышестоящего руководства. Однако наиболее вероятна ситуация передачи инцидента ИБ непосредственно в ГРИИБ для дальнейшей оценки и выполнения соответствующих действий.

9.6.1.4. Каким бы ни был следующий шаг, сотрудник группы обеспечения эксплуатации должен заполнить форму отчета по возможности наиболее подробно. Отчет должен содержать информацию в описательном виде и, насколько это возможно, характеризовать:

- что представляет собой инцидент ИБ;

- что явилось его причиной, чем или кем он был вызван;

- на что он влияет или может повлиять;

- реальное или потенциальное воздействие инцидента ИБ на бизнес организации;

- указание на вероятную значительность или незначительность инцидента ИБ (по шкале серьезности, принятой в организации);

- как инцидент ИБ обрабатывался до этого времени.

9.6.1.5. При рассмотрении потенциального или фактического негативного воздействия инцидента на бизнес организации в результате несанкционированного раскрытия информации, несанкционированной модификации информации, отказа от имеющейся информации, недоступности информации и (или) сервиса, уничтожения информации и (или) сервиса в первую очередь необходимо определить, какое из перечисленных ниже последствий будет иметь инцидент ИБ.

Примерами последствий ИБ являются:

- финансовые убытки/прерывание бизнес-операций;

- ущерб коммерческим и экономическим интересам;

- ущерб информации, содержащей персональные данные;

- нарушение правовых и нормативных обязательств;

- сбои операций по менеджменту и бизнес-операций;

- утрата престижа организации.

9.6.1.6. Для категорий, отнесенных к инциденту ИБ, должны использоваться соответствующие рекомендации по категорированию потенциальных или фактических воздействий для внесения их в отчет по инцидентам ИБ.

9.6.1.7. Если инцидент ИБ был разрешен, то отчет должен содержать детали предпринятых защитных мер и извлеченных уроков (например, защитные меры, которые должны быть приняты для предотвращения повторного появления подобных инцидентов ИБ).

9.6.1.8. После наиболее подробного, по мере возможности, заполнения форма отчета должна быть представлена в ГРИИБ для ввода в базу данных инцидентов и событий ИБ и анализа в будущем.

9.6.1.9. Если расследование проводится больше недели, то должен быть составлен промежуточный отчет.

9.6.1.10. Важно, чтобы сотрудник группы обеспечения эксплуатации, оценивающий инцидент ИБ, основываясь на руководстве, содержащемся в документации системы менеджмента инцидентов ИБ, был осведомлен о том:

- когда и кому необходимо направлять материалы об инциденте;

- что при осуществлении всех действий, выполняемых группой обеспечения эксплуатации, необходимо выполнять документированные процедуры контроля изменений.

9.6.1.11. При наличии проблем или мнения о том, что существуют проблемы с установленными по умолчанию механизмами электронного оповещения (например электронной почтой), включая случаи атаки на информационную систему и считывание несанкционированными лицами формы отчета об инцидентах ИБ, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть: телефон, текстовые сообщения, а также курьеры. Такие альтернативные средства должны использоваться на ранних стадиях расследования, когда становится очевидным, что событие ИБ будет переведено в категорию инцидента ИБ, особенно такого инцидента ИБ, который может считаться "значительным".

9.6.2. Вторая оценка и подтверждение инцидента информационной безопасности. Вторая оценка и подтверждение инцидента ИБ или какое-либо другое решение относительно того, надо ли отнести событие ИБ к инциденту ИБ, должны входить в обязанности ГРИИБ. Принимающий отчеты сотрудник ГРИИБ должен:

- подтвердить получение формы отчета, заполненной по возможности наиболее подробно, группой обеспечения эксплуатации;

- ввести эту форму в базу данных событий/инцидентов ИБ;

- обратиться за уточнениями к группе обеспечения эксплуатации;

- проанализировать содержание отчетной формы;

- собрать дополнительную необходимую информацию о событии ИБ (если существует) от группы обеспечения эксплуатации, лица, заполнившего отчетную форму, или из какого-либо иного источника.

9.6.2.1. Если все еще остается какая-либо неопределенность относительно аутентичности инцидента ИБ или полноты полученной информации, то сотрудник ГРИИБ должен провести вторую оценку для определения реальности или ложности инцидента ИБ. Если инцидент ИБ определен как ложный, необходимо заполнить отчет о событии ИБ, добавить его в базу данных событий/инцидентов ИБ и передать руководителю ГРИИБ. Копии отчета необходимо передать группе обеспечения эксплуатации, лицу, сообщившему о событии, и его/ее местному руководителю.

9.6.2.2. Если инцидент ИБ определяется как реальный, то сотрудник ГРИИБ, при необходимости привлекая коллег, должен провести дальнейшую оценку. Целью оценки является максимально быстрое подтверждение:

- того, что представляет собой инцидент ИБ, что явилось его причиной, чем или кем был вызван, на что повлиял или мог повлиять, воздействие или потенциальное воздействие инцидента ИБ на бизнес организации, указание на вероятную значительность/незначительность инцидента (по шкале серьезности инцидентов, принятой в организации);

- предумышленной технической атаки нарушителя на некоторую информационную систему, сервис и (или) сеть, например:

глубины проникновения нарушителя в систему, сервис и (или) сеть и степень контроля, которой он обладает;

данных об информации, к которой получил доступ нарушитель, были ли они скопированы, изменены или удалены;

о том, какое программное обеспечение было скопировано, изменено или разрушено нарушителем;

в отношении предумышленной физической атаки нарушителя на любую информационную систему аппаратной части, сервиса и (или) на сеть и (или) на физическое месторасположение, например:

масштаба прямых и косвенных последствий нанесенного физического ущерба (при отсутствии физической защиты доступа);

прямых и косвенных последствий в отношении инцидентов ИБ, косвенно созданных действиями нарушителя (например, стал ли физический доступ возможным по причине пожара, является ли уязвимость информационной системы следствием неправильного функционирования программного обеспечения, линии связи или ошибки оператора);

- используемого до настоящего времени способа обработки инцидента ИБ.

9.6.2.3. При анализе потенциального или реального негативного воздействия инцидента ИБ на бизнес организации вследствие несанкционированного раскрытия информации, несанкционированной модификации информации, отказа от имеющейся информации, недоступности информации и (или) сервиса, разрушения информации и (или) сервиса необходимо подтвердить, какие последствия имели место вследствие данного инцидента. Примерами категорий последствий являются:

- финансовые убытки/разрушение бизнес-операций;

- ущерб коммерческим и экономическим интересам;

- ущерб для информации, содержащей персональные данные;

- нарушение правовых и нормативных обязательств;

- ущерб для менеджмента и бизнес-операций;

- утрата престижа организации.

9.6.2.4. Для отнесения потенциальных или фактических воздействий к той или иной категории необходимо использовать соответствующие рекомендации, которые относили бы их к инциденту ИБ и вносились в отчет по инцидентам ИБ.

9.7. Реагирование на инциденты.

9.7.1. Немедленное реагирование.

9.7.1.1. В большинстве случаев после подтверждения инцидента член ГРИИБ выполняет действия по немедленному реагированию относительно инцидента ИБ, регистрации подробностей в форме отчета об инциденте ИБ, введению в базу данных событий/инцидентов ИБ и уведомлению сотрудников организации о требуемых действиях на инцидент ИБ. Результатом данных действий может быть принятие аварийных защитных мер (например, отключение атакованной информационной системы, сервиса и (или) сети по предварительному соглашению с соответствующим руководством ИТ-подразделения и (или) бизнес-руководством) и (или) определение дополнительных постоянных защитных мер и уведомление сотрудников организации о принятии этих мер. Если аварийные защитные меры не применены, то нужно определить значительность инцидента ИБ по оценочной шкале, принятой в организации, и если инцидент ИБ достаточно значителен, то об этом необходимо непосредственно уведомить соответствующее вышестоящее руководство. Если очевидна необходимость объявления кризисной ситуации, руководитель, отвечающий за обеспечение непрерывности бизнеса, должен быть оповещен о возможной активизации плана обеспечения непрерывности бизнеса, причем необходимо проинформировать руководителя ГРИИБ и вышестоящее руководство.

9.7.1.2. Примерные действия по реагированию. Примером действий по немедленному реагированию в случае преднамеренной атаки на информационную систему, сервис и (или) сеть может быть то, что они остаются подключенными к Интернету и другим сетям с целью:

- обеспечения правильного функционирования критически важных бизнес-приложений;

- сбора наиболее полной информации о нарушителе при условии, если он не знает, что находится под наблюдением.

Однако при принятии решения по реагированию нужно учитывать следующие факторы:

- нарушитель может почувствовать, что находится под наблюдением, и предпринять действия, наносящие дальнейший ущерб атакованной системе, сервису и (или) сети и данным;

- нарушитель может разрушить информацию, которая способствует его отслеживанию.

9.7.1.2.1. Предотвращение повторного проявления инцидента обычно является более приоритетной задачей. В некоторых случаях необходимо учитывать то, что нарушитель выявил слабое место, которое должно быть устранено, а выгоды от выявления нарушителя не оправдывают затраченных на это усилий. Это особенно справедливо, если нарушитель на самом деле не является злоумышленником и не нанес большого или вообще не причинил никакого ущерба.

9.7.1.2.2. Что касается других инцидентов ИБ, кроме преднамеренной атаки, то их источник должен быть идентифицирован. Может потребоваться отключение информационной системы, сервиса и (или) сети или изоляция соответствующих их частей после получения предварительного согласия соответствующего руководства ИТ и (или) бизнес-руководителя на время внедрения защитных мер. Для этого может потребоваться больше времени, если уязвимое место для информационной системы, сервиса и (или) для сети окажется существенным или критически важным.

9.7.1.2.3. Другим действием по реагированию может быть активизация методов наблюдения. Это действие должно осуществляться на основе процедур, документированных для системы менеджмента инцидентов ИБ.

9.7.1.2.4. Информация, которая могла быть повреждена в результате инцидента ИБ, должна быть проверена членом ГРИИБ по резервным записям на предмет изменения, стирания или модификации информации. Может возникнуть необходимость проверки целостности журналов регистрации, поскольку злонамеренный нарушитель может подделать их с целью сокрытия следов проникновения.

9.7.1.3. Обновление информации об инцидентах. Независимо от последующих действий, сотрудник ГРИИБ должен обновить отчет об инциденте ИБ с максимальной детализацией, добавить его в базу данных событий/инцидентов ИБ, оповестив об этом руководителя ГРИИБ и (при необходимости) других лиц. Обновляют следующую информацию:

- о том, что представляет собой инцидент ИБ;

- о том, что явилось причиной, чем или кем он был вызван;

- на что воздействует или мог воздействовать;

- о фактическом или потенциальном воздействии инцидента ИБ на бизнес организации;

- об изменениях в указании на вероятную значительность или незначительность инцидента ИБ (по шкале серьезности, принятой в организации);

- о том, как он обрабатывался до этого времени.

9.7.1.3.1. Если инцидент ИБ разрешен, то отчет должен содержать подробности предпринятых защитных мер и извлеченных уроков (например, дополнительные защитные меры, которые следует предпринять для предотвращения повторного появления данного инцидента ИБ или подобных ему инцидентов ИБ). Обновленный отчет следует добавлять в базу данных событий/инцидентов ИБ и уведомлять руководителя ГРИИБ и других лиц по их требованию.

9.7.1.3.2. ГРИИБ отвечает за обеспечение безопасного хранения информации, относящейся к данному инциденту ИБ, с целью возможного проведения дальнейшей экспертизы и возможного использования судом в качестве доказательства. Например, для инцидента ИБ, ориентированного на ИТ, после первоначального обнаружения инцидента ИБ все непостоянные данные должны быть собраны до отключения пораженной системы ИТ, сервиса и (или) сети до проведения судебного расследования. Предназначенная для сбора информация содержит сведения о любых функционирующих процессах и хранится в памяти, кеше и регистрах. При этом необходимо:

- в зависимости от характера инцидента ИБ провести полное дублирование пораженной системы, сервиса и (или) сети на случай судебного разбирательства или резервное копирование журналов и важных файлов;

- собрать и проанализировать журналы соседних систем, сервисов и (или) сетей, например, маршрутизаторов и межсетевых экранов;

- всю собранную информацию хранить на носителях только для чтения;

- при выполнении дублирования на случай судебного разбирательства обеспечить присутствие не менее двух лиц для утверждения и подтверждения того, что все действия были выполнены согласно действующему нормативному законодательству;

- документировать и хранить вместе с исходными носителями спецификации и описания сервисных команд, которые используются для дублирования на случай судебного разбирательства.

9.7.1.3.3. Член ГРИИБ также является ответственным, если это возможно, во время обновления информации об инцидентах ИБ за возвращение в безопасное рабочее состояние пораженных устройств (имеющих или не имеющих отношение к ИТ) в интересах исключения атак на эти устройства.

9.7.1.4. Дополнительные действия. При определении членом ГРИИБ реальности инцидента ИБ его дополнительными действиями должны быть:

- проведение правовой экспертизы;

- информирование лиц, ответственных за передачу информации внутри организации и за ее пределами, о фактах и предложениях по информации, которую надо передать, в какой форме и кому.

9.7.1.4.1. После возможно наиболее подробного заполнения отчета об инциденте ИБ отчет вводится в базу данных событий/инцидентов ИБ и передается руководителю ГРИИБ.

9.7.1.4.2. Если время расследования превышает время, ранее согласованное внутри организации, то составляется промежуточный отчет.

9.7.1.4.3. Член ГРИИБ, оценивающий инцидент ИБ, на основании руководства, содержащегося в документации системы менеджмента инцидентов ИБ, должен знать:

- когда и кому необходимо направлять материалы;

- что при осуществлении любой деятельности ГРИИБ необходимо следовать документированным процедурам контроля за внесением изменений.

9.7.1.4.4. При наличии проблем или если считается, что существуют проблемы в отношении обычных средств связи (например, с электронной почтой), включая случаи, когда система, возможно, подвергается атаке и целесообразно сделать вывод, что инцидент ИБ является значительным и (или) была определена кризисная ситуация, то следует в первую очередь сообщить об инциденте ИБ ответственным лицам лично, по телефону или текстовым сообщением.

9.7.1.4.5. При необходимости руководитель ГРИИБ совместно с руководителем обеспечения безопасности ИБ организации и соответствующим руководителем организации (членом совета директоров) правления должны связаться со всеми отделами, которые вовлечены в инцидент ИБ как внутри организации, так и за ее пределами.

9.7.1.4.6. Для быстрой и эффективной организации связи необходимо заранее установить надежный метод передачи информации, не зависящий полностью от системы, сервиса или сети, на которые может воздействовать инцидент ИБ. Такие меры предосторожности могут включать в себя назначение резервных консультантов или представителей организации на случай отсутствия кого-либо из ее основных руководителей.

9.7.2. Контролируемость инцидента. После инициирования членом ГРИИБ немедленного реагирования соответствующей правовой экспертизы и действий по передаче информации необходимо срочно убедиться, находится ли инцидент ИБ под контролем. При необходимости член ГРИИБ может проконсультироваться с коллегами, руководителем ГРИИБ и (или) другими сотрудниками организации.

9.7.2.1. Если подтверждается, что инцидент ИБ находится под контролем, то член ГРИИБ должен перейти к другим дальнейшим необходимым действиям по реагированию, проведению правовой экспертизы и передаче информации с целью ликвидации инцидента ИБ и восстановления нормальной работы пораженной информационной системы.

9.7.2.2. Если не подтверждается, что инцидент ИБ находится под контролем, член ГРИИБ должен инициировать антикризисные действия.

9.7.3. Последующее реагирование. Определив, что инцидент ИБ находится под контролем и не является объектом антикризисной ситуации, член ГРИИБ должен определить необходимость и вероятные способы дальнейшего реагирования в отношении данного инцидента. Реагирование может включать в себя восстановление пораженных информационных систем(ы), сервисов(а) и (или) сетей(и) до нормального рабочего состояния. Затем член ГРИИБ должен занести детали в форму отчета об инциденте ИБ и базу данных событий/инцидентов ИБ, а также проинформировать об этом лиц, ответственных за завершение соответствующих действий. Подробности успешного завершения этих действий необходимо внести в форму отчета об инциденте ИБ и базу данных событий/инцидентов ИБ, а затем инцидент ИБ должен быть закрыт и соответствующий персонал должен быть проинформирован об этом.

9.7.3.1. Некоторые реагирования должны быть направлены на предотвращение повторения подобного ему инцидента ИБ. Например, если определено, что причиной инцидента ИБ является отказ аппаратурной части или программного обеспечения ИТ из-за отсутствия вставок в программу ("патчей"), то в этом случае необходимо немедленно связаться с поставщиком. Если причиной инцидента ИБ была известная уязвимость ИТ, то она должна быть устранена соответствующим обновлением защиты ИБ. Необходимо также решить любые проблемы, связанные с конфигурацией ИТ и выявленным инцидентом ИБ. Другими мерами уменьшения возможности повторения или появления такого инцидента ИБ или подобного ему инцидента могут быть изменение системных паролей и отключение неиспользуемых сервисов.

9.7.3.2. Другая область деятельности по реагированию на инцидент ИБ может включать в себя мониторинг системы, сервиса и (или) сети ИТ. Следом за оценкой инцидента ИБ может оказаться целесообразным ввести дополнительные защитные меры мониторинга для содействия в обнаружении необычных или подозрительных событий, которые могут оказаться признаками инцидентов ИБ. Такой мониторинг поможет также глубже раскрыть инцидент ИБ и идентифицировать другие системы ИТ, которые подверглись компрометации.

9.7.3.3. Может возникнуть необходимость в активизации специальных реагирований, документированных в соответствующем плане обеспечения непрерывности бизнес-процесса, которые можно применить к инцидентам ИБ как связанным, так и не связанным с ИТ. Специальные реагирования должны быть предусмотрены для всех аспектов бизнеса, связанных не только непосредственно с ИТ, но также с поддержкой ключевых функций бизнеса и последующего восстановления с помощью речевой сети связи и физических устройств.

9.7.3.4. Еще одной областью реагирования является восстановление пораженных информационных систем(ы), сервисов(а) и (или) сетей(и) до нормального рабочего состояния. Восстановление пораженных систем(ы), сервисов(а) и (или) сетей(и) до безопасного рабочего состояния может быть осуществлено применением "патчей" для известных уязвимостей или отключением скомпрометированных элементов. Если вследствие уничтожения журналов регистрации во время действия инцидента ИБ исчезает весь объем информации об инциденте ИБ, может потребоваться полная перестройка системы, сервиса и (или) сети. Также может потребоваться активизация части соответствующего плана непрерывности бизнеса.

9.7.3.5. Если инцидент ИБ, не связанный с ИТ, например, спровоцирован пожаром, наводнением или взрывом, то выполняются действия по восстановлению, документированные в соответствующем плане обеспечения непрерывности бизнеса.

9.7.4. Антикризисные действия. Может случиться так, что при определении ГРИИБ контролируется ли инцидент ИБ, группа придет к выводу, что инцидент ИБ не находится под контролем и должен обрабатываться в режиме антикризисных действий. В этом случае используется предварительно разработанный план (планы).

9.7.4.1. Лучшие варианты обработки всех возможных типов инцидентов ИБ, которые могут повлиять на доступность/разрушение и, в некоторой степени, на целостность информационной системы, должны быть определены в стратегии обеспечения непрерывности бизнеса организации. Эти варианты должны быть непосредственно связаны с приоритетами бизнеса организации и

соответствующими временными рамками восстановления бизнес-процессов и, следовательно, с максимально приемлемым временем простоя ИТ, речевой связи, персонала и размещения. В плане необходимо определить:

- предупреждающие, поддерживающие меры обеспечения непрерывности бизнеса и устойчивости к внешним изменениям;

- организационную структуру и обязанности, связанные с управлением планирования непрерывности бизнеса;

- структуру и основные положения плана (планов) обеспечения непрерывности бизнеса.

9.7.4.2. План (планы) обеспечения непрерывности бизнеса и защитные меры для поддержки активизации этого (этих) плана (планов), протестированных и признанных удовлетворительными, должны создать основу для ведения наиболее антикризисных действий, для которых они предназначены.

9.7.4.3. Другие типы возможных антикризисных действий включают в себя (но не ограничиваются) активизацией:

- средств пожаротушения и процедур эвакуации;

- средств предотвращения наводнения и процедур эвакуации;

- средств предотвращения взрыва бомбы и соответствующих процедур эвакуации;

- работы специалистов по расследованию фактов мошенничества в информационных системах;

- работы специалистов по расследованию технических атак.

9.7.5. Правовая экспертиза. Если в ходе предыдущей оценки была определена необходимость правовой экспертизы в целях доказательства значительного инцидента ИБ, правовую экспертизу проводит ГРИИБ. В целях проведения более подробной экспертизы конкретного инцидента ИБ необходимо применять следственные методы и средства, основанные на ИТ и поддерживаемые документированными процедурами, не используемые ранее в процессе менеджмента инцидентов ИБ. Такую экспертизу проводят структурным методом и определяют, что может использоваться в качестве доказательства при внутренних дисциплинарных разбирательствах или в ходе судебных процессов.

9.7.5.1. Для проведения правовой экспертизы могут использоваться технические (например, средства и методы аудита, средства восстановления свидетельств) и программные средства, защищенные служебные помещения, а также соответствующий персонал. Каждое действие правовой экспертизы должно быть полностью документировано, включая представление соответствующих фотографий, составление отчетов об анализе результатов аудита, проверку журналов восстановления данных. Квалификация лица или лиц, проводившего(их) правовую экспертизу, должна быть документирована так же, как результаты квалификационного тестирования. Необходимо также документировать любую другую информацию, способную продемонстрировать объективность и логический характер правовой экспертизы. Все записи о самих инцидентах ИБ, деятельности, связанной с правовой экспертизой этих инцидентов, и т.д., а также соответствующие носители информации должны храниться в физически защищенной среде и контролироваться соответствующими процедурами для предотвращения доступа к ним неавторизованных лиц с целью модификации записей. Средства правовой экспертизы, основанные на применении ИТ, должны точно соответствовать правовым нормам с целью исключения возможности оспаривания этого соответствия в судебном порядке и, в то же время, в них должны учитываться все текущие изменения в технологиях. В физической среде ГРИИБ необходимо создавать необходимые условия, гарантирующие неоспоримость обработки свидетельств. В любое время для обеспечения реагирования на инцидент ИБ число персонала должно быть достаточным.

9.7.5.2. Со временем, несомненно, возникнет необходимость разработки требований к анализу свидетельств в контексте многообразия инцидентов ИБ, включая мошенничество, кражу и акты вандализма. Следовательно, для содействия ГРИИБ потребуется большее число средств, основанных на ИТ, и вспомогательных процедур для раскрытия информации, скрытой в информационной системе, сервисе и (или) сети, включая информацию, которая на первый взгляд кажется стертой, зашифрованной или поврежденной. Эти средства должны учитывать все аспекты, связанные с известными типами инцидентов ИБ (разумеется, они должны быть документированы в процедурах ГРИИБ).

9.7.5.3. В современных условиях в правовую экспертизу часто включают сложные среды с сетевой структурой, в которых расследование распространяется на всю операционную среду, включая множество серверов (файловый сервер, серверы печати, связи, электронной почты и т.д.), а также средства удаленного доступа. Существует много инструментальных средств, включая средства поиска текстов, программное обеспечение формирования изображений и пакеты программ для правовой экспертизы. Главной целью процедур правовой экспертизы является сохранение свидетельств в неприкосновенности, их проверка на предмет противостояния любым оспариваниям в суде и проведение правовой экспертизы на точной копии исходных данных с тем, чтобы избежать сомнений в целостности исходных носителей в ходе аналитической работы.

9.7.5.4. Общий процесс правовой экспертизы должен охватывать следующие виды деятельности:

- обеспечение защиты целевой системы, сервиса и (или) сети в процессе проведения правовой экспертизы от превращения их в недоступные, изменения или от иной компрометации, включая введение вирусов, и обеспечение защиты от воздействий или минимальных воздействий на их нормальную работу;

- назначение приоритетов сбора доказательств, то есть рассмотрение их от наиболее до наименее изменчивых (что в значительной степени зависит от характера инцидента ИБ);

- идентификация всех необходимых файлов в предметной системе, сервисе и (или) сети, включая нормальные файлы, файлы, кажущиеся уничтоженными, но не являющиеся таковыми, файлы, защищенные паролем или иным образом, и зашифрованные файлы;

- восстановление как можно большего числа стертых файлов и других данных;

- раскрытие IP-адресов, имен хостов, сетевых маршрутов и информации Web-сайтов;

- извлечение содержимого скрытых, временных файлов и файлов подкачки, используемых как программное обеспечение операционной системы, так и как прикладное программное обеспечение;

- доступ к содержимому программного обеспечения защищенных или зашифрованных файлов (если это не запрещено законодательством);

- анализ всех возможно значимых данных, найденных в специальных (обычно недоступных) областях памяти на дисках;

- анализ времени доступа к файлу, его создания и изменения;

- анализ журналов регистрации системы/сервиса/сети и приложений;

- определение деятельности пользователей и (или) приложений в системе/сервисе/сети;

- анализ электронной почты на наличие исходной информации и ее содержания;

- проведение проверок целостности файлов с целью обнаружения файлов, содержащих "Троянского коня", и файлов, изначально отсутствовавших в системе;

- по возможности анализ физических доказательств ущерба имуществу, например отпечатков пальцев, результатов видеонаблюдения, журналов регистрации системы сигнализации, журналов регистрации доступа по пропускам и опроса свидетелей;

- обработка и хранение добытых потенциальных свидетельств так, чтобы избежать их повреждения, приведения в негодность и предотвращения просмотра конфиденциального материала несанкционированными лицами. Следует подчеркнуть, что сбор доказательств всегда должен проводиться в соответствии с правилами судопроизводства или слушания дела, для которых возможно представление данного доказательства;

- получение выводов о причинах инцидента ИБ, необходимых действиях и времени их выполнения с приведением свидетельств, включая список соответствующих файлов, включенных в приложение к главному отчету;

- обеспечение экспертной поддержки для любого дисциплинарного или правового действия (при необходимости).

Метод(ы) выполнения вышеуказанных действий должен(ны) документироваться в работе процедуры ГРИИБ.

X. ПРИМЕРЫ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРИЧИН ИХ ВОЗНИКНОВЕНИЯ

10.1. Инциденты ИБ могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или природных явлений) и вызваны как техническими, так и нетехническими средствами. Их последствиями могут быть такие события, как несанкционированные раскрытие или изменение информации, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам организации или их хищение. Инциденты ИБ, о которых не было сообщено, но которые были определены как инциденты, расследовать невозможно и защитных мер для предотвращения повторного появления этих инцидентов применить нельзя. Важно заметить, что эти примеры не являются исчерпывающими.

10.2. Отказ в обслуживании. Отказ в обслуживании является обширной категорией инцидентов ИБ, имеющих одну общую черту. Подобные инциденты ИБ приводят к неспособности систем, сервисов или сетей продолжать функционирование с прежней производительностью, чаще всего при полном отказе в доступе авторизованным пользователям.

10.2.1. Существует два основных типа инцидентов ИБ, связанных с отказом в обслуживании, создаваемых техническими средствами: уничтожение ресурсов и истощение ресурсов. Некоторыми типичными примерами таких преднамеренных технических инцидентов ИБ "отказ в обслуживании" являются:

- зондирование сетевых широковещательных адресов с целью полного заполнения полосы пропускания сети трафиком ответных сообщений;

- передача данных в непредусмотренном формате в систему, сервис или сеть в попытке разрушить или нарушить их нормальную работу;

- одновременное открытие нескольких сеансов с конкретной системой, сервисом или сетью в попытке исчерпать их ресурсы (то есть замедление их работы, блокирование или разрушение).

10.2.2. Отказ в обслуживании в результате ошибки в конфигурации, допущенной оператором, или из-за несовместимости прикладного программного обеспечения.

10.2.3. Отказ в обслуживании инициированный намеренно с целью разрушения системы, сервиса и снижения производительности сети.

10.2.4. Многие преднамеренные технические инциденты типа "отказ в обслуживании" часто инициируются анонимно (то есть источник атаки неизвестен), поскольку злоумышленник обычно не получает информации об атакуемой сети или системе.

10.2.5. Инциденты ИБ "отказ в обслуживании", создаваемые нетехническими средствами и приводящие к утрате информации, сервиса и (или) устройств обработки информации, могут вызываться:

- нарушениями систем физической защиты, приводящими к хищениям, преднамеренному нанесению ущерба или разрушению оборудования;

- случайным нанесением ущерба аппаратуре и (или) ее местоположению от огня или воды/наводнения;

- экстремальными условиями окружающей среды, например высокой температурой (вследствие выхода из строя системы кондиционирования воздуха);

- неправильным функционированием или перегрузкой системы;

- неконтролируемыми изменениями в системе;

- неправильным функционированием программного или аппаратного обеспечения.

10.3. Сбор информации. Подобные инциденты ИБ предполагают проведение разведки с целью определения:

- наличия цели, получения представления об окружающей ее сетевой топологии и о том, с кем обычно эта цель связана обменом информации;

- потенциальных уязвимостей цели или непосредственно окружающей ее сетевой среды, которые можно использовать для атаки.

Типичными примерами атак, направленных на сбор информации техническими средствами, являются:

- сбрасывание записей DNS (системы доменных имен) для целевого домена Интернета (передача зоны DNS);

- отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы;

- зондирование системы с целью идентификации (например, по контрольной сумме файлов) операционной системы хоста;

- сканирование доступных сетевых портов на протокол передачи файлов системе с целью идентификации соответствующих сервисов (например электронная почта, протокол FTP, сеть и т.д.) и версий программного обеспечения этих сервисов;

- сканирование одного или нескольких сервисов с известными уязвимостями по диапазону сетевых адресов (горизонтальное сканирование).

10.3.1. В некоторых случаях технический сбор информации расширяется и переходит в несанкционированный доступ, если, злоумышленник при поиске уязвимости пытается получить несанкционированный доступ. Обычно это осуществляется автоматизированными средствами взлома, которые не только производят поиск уязвимости, но и автоматически пытаются использовать уязвимые системы, сервисы и (или) сети.

10.3.2. Инциденты, направленные на сбор информации, создаваемые нетехническими средствами, приводят:

- к прямому или косвенному раскрытию или модификации информации;

- хищению интеллектуальной собственности, хранимой в электронной форме;

- нарушению учета, например, при регистрации учетных записей;

- неправильному использованию информационных систем (например, с нарушением закона или политики организации).

Инциденты могут вызываться, например, следующими факторами:

- нарушениями физической защиты безопасности, приводящими к несанкционированному доступу к информации и хищению устройств хранения данных, содержащих значимые данные, например ключи шифрования;

- неудачно и (или) неправильно конфигурированными операционными системами по причине неконтролируемых изменений в системе или неправильным функционированием программного или аппаратного обеспечения, приводящим к тому, что персонал организации или посторонний персонал получает доступ к информации, не имея на это разрешения.

10.4. Несанкционированный доступ. Примеры несанкционированного доступа с помощью технических средств включают в себя:

- попытки извлечь файлы с паролями;

- атаки переполнения буфера с целью получения привилегированного (например, на уровне системного администратора) доступа к сети;

- использование уязвимостей протокола для перехвата соединения или ложного направления легитимных сетевых соединений;

- попытки расширить привилегии доступа к ресурсам или информации по сравнению с легитимно имеющимися у пользователя или администратора.

Инциденты несанкционированного доступа, создаваемые нетехническими средствами, которые приводят к прямому или косвенному раскрытию или модификации информации, нарушениям учета или неправильному использованию информационных систем, могут вызываться следующими факторами:

- разрушением устройств физической защиты с последующим несанкционированным доступом к информации;

- неудачной и (или) неправильной конфигурацией операционной системы вследствие неконтролируемых изменений в системе или неправильного функционирования программного или аппаратного обеспечения.

XI. РАЗРАБОТКА И ТЕСТИРОВАНИЕ КОМПЛЕКСА ПРОГРАММНЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ, УСЛУГ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

11.1. После того как специализированная архитектура безопасности полностью документально оформлена и согласована, включая одобрение высшего руководства, должен быть разработан комплекс программных и технических средств и услуг по обеспечению безопасности, который должен быть реализован в экспериментальном режиме, тщательно протестирован, и должна быть проведена проверка его соответствия.

11.2. Общая проверка комплекса программных и технических средств и услуг на соответствие назначению должна проводиться в соответствии с документацией по стратегии тестирования, описывающей метод тестирования и позволяющей испытывать комплекс

программных и технических средств и услуг, и планом тестирования. В результате идентификации недостатков в ходе такого тестирования могут потребоваться внесение изменения и проведение любого необходимого повторного тестирования.

11.3. После того как тестирование на соответствие назначению успешно проведено и осуществлены какие-либо необходимые изменения, должна быть проведена проверка реализации на предмет соответствия документированной специализированной архитектуры безопасности необходимым мерам и средствам контроля и управления безопасностью, определенным в следующих документах:

- специализированная архитектура безопасности;

- политика сетевой безопасности;

- документы, связанные с SecOPs;

- политика (безопасности) доступа к услуге шлюза безопасности;

- план(ы) обеспечения непрерывности деятельности;

- условия обеспечения безопасности соединения (при необходимости).

11.4. Проверка соответствия комплекса программных и технических средств и услуг должна проводиться до начала фактического функционирования. Проверка комплекса программных и технических средств и услуг будет завершена, когда все недостатки идентифицированы, исправлены и признаны высшим руководством.

11.5. Проверка соответствия комплекса программных и технических средств и услуг должна включать в себя проведение тестирования безопасности по соответствующим национальным стандартам, стандартам организации (в отсутствие национальных стандартов) в соответствии с заранее разработанной стратегией тестирования безопасности и связанными с ней планами тестирования безопасности, точно определяющими, какое тестирование должно проводиться, с помощью чего, где и когда (примерный образец плана тестирования безопасности приведен в ИСО/МЭК 27033-2). Обычно тестирование должно сочетать в себе поиск уязвимостей и тестирование на проникновение. Перед началом любого такого тестирования необходимо проверить план тестирования с тем, чтобы обеспечить уверенность в проведении тестирования в полном соответствии с релевантными законодательством и инструкциями. При проведении этой проверки не следует забывать о том, что сеть может не ограничиваться одной страной, а распространяться на другие страны с различными законодательствами. После проведения тестирования в отчетах должны указываться особенности обнаруженных уязвимостей, необходимые меры по их устранению, и приоритет их принятия, а в приложении должно подтверждаться, что все согласованные меры по их устранению применены. Такие отчеты должны быть подписаны высшим руководством организации.

11.6. Когда все результаты будут признаны удовлетворительными, реализация должна быть одобрена и принята, включая одобрение высшего руководства организации.

XII. МОНИТОРИНГ И ПРОВЕРКА ЭКСПЛУАТАЦИИ КОМПЛЕКСА ПРОГРАММНЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ И УСЛУГ

После начала эксплуатации должны проводиться действия по текущему мониторингу и проверке соответствия требованиям национальных стандартов, стандартов организации (при отсутствии национальных стандартов). Такие мероприятия должны проводиться ежегодно до появления новой основной версии (комплекса программных и технических средств и услуг), связанной со значительными изменениями потребностей деятельности организации, технологии, решений по обеспечению безопасности и т.д.

XIII. ОТВЕТСТВЕННОСТЬ

Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.